Network Coding for Security and Error Correction

NGAI, Chi Kin

A Thesis Submitted in Partial Fulfilment
of the Requirements for the Degree of
Doctor of Philosophy
in
Information Engineering

©The Chinese University of Hong Kong
July 2008

The Chinese University of Hong Kong holds the copyright of this thesis. Any person(s) intending to use a part or whole of the materials in the thesis in a proposed publication must seek copyright release from the Dean of the Graduate School.

Abstract of thesis entitled:

Network Coding for Security and Error Correction

Submitted by NGAI, Chi Kin

for the degree of Doctor of Philosophy

at The Chinese University of Hong Kong in July 2008

Network coding is one of the most important breakthroughs in information theory in recent years. The theory gives rise to a new concept regarding the role of nodes in a communication network. Unlike in existing networks where the nodes act as switches, in the paradigm of network coding, every node in the network can act as an encoder for the incoming information. With this new infrastructure, it is possible to utilize the full capacity of the network where it is impossible to do so without network coding. In the seminar paper by Ahlswede et al. [1] where network coding was introduced, the achievability of the max-flow bound for every single source multicast network by using network coding was also proved. By further exploring the possibility of linear network coding, Cai and Yeung introduced the idea of error-correcting network coding and secure network coding in [5] and [18] respectively. These papers launched another two important research areas in the field of network coding.

In this work, we consider the possibility and the effectiveness of implementing secure network coding and error-correcting network coding at the same time. Upon achieving this goal, information can be multicast securely to the sink nodes through a noisy network. Toward this end, we propose constructions of such codes and prove their optimality. After that, we extend the idea of generalized Hamming Weight [9] for the classical point-to-point communication channel to linear network coding. We also extend the idea of generalized Singleton bound to linear network coding. We further show that the generalized Hamming weight can completely characterize the security performance of linear code at the source node on a given linear network code. We then introduce the idea of Network Maximum Distance Separable code (NMDS code), which can be shown to play an important role in minimizing the information that an eavesdropper can obtain from the network. The problem of obtaining the optimal security performance is in fact equivalent to the problem of obtaining a Network Maximum Distance Separable code.

Acknowledgement

I want to thank my supervisor Prof. Raymond Wai-Ho Yeung for his resourceful guidance on my research process. It is Prof. Yeung who suggested the theme of this thesis and provided me with the best environment throughout the whole project. Without his support and advice on writing and presentation skills, it would be much more difficult for me to complete the project. This thesis would not have been possible without his valuable ideas and support. I also want to thanks my dearest TAs and friends, Ting, Shue, Wai, Shenghao, Zhixue and Crystal who gave me lots of support all along the way not only on the research but also in sharing my pressure while I was dull and anxious. Without them, it would be much more difficult for me to handle the time while I felt helpless and lonely.

To mammy, my family, Crystal,
and people who give me support all along the way

Contents

List of Figures

Chapter 1

Introduction

Summary

The aim of this chapter is to give a brief introduction of network coding and linear network coding which are originated in [1] and [2] respectively. In this chapter, point-to-point communication network on which one information source is to be transmitted to certain sets of sinks are considered. It can be seen by employing coding at the nodes that bandwidth can in general be increased over the traditional replication and forward scheme. Among the simplest coding schemes is linear coding, which regards a block of data as a vector over a certain base field and allows a node to apply a linear transformation to a vector before passing it on. It can be proved that linear network coding suffices to achieve the optimum of all single information source multicast problem.

In a point-to-point communication system, the transmitting point and the receiving point are connected by a communication channel. An information source is generated at the transmission point, and the purpose of the communication system is to deliver the information generated at the transmission point to the receiving point via the channel. In a multicast network, data is to be transmitted from the source node to a prescribed set of destination nodes. Given the transmission requirements, a natural question is whether the network can fulfill these requirements and how it can be done efficiently.

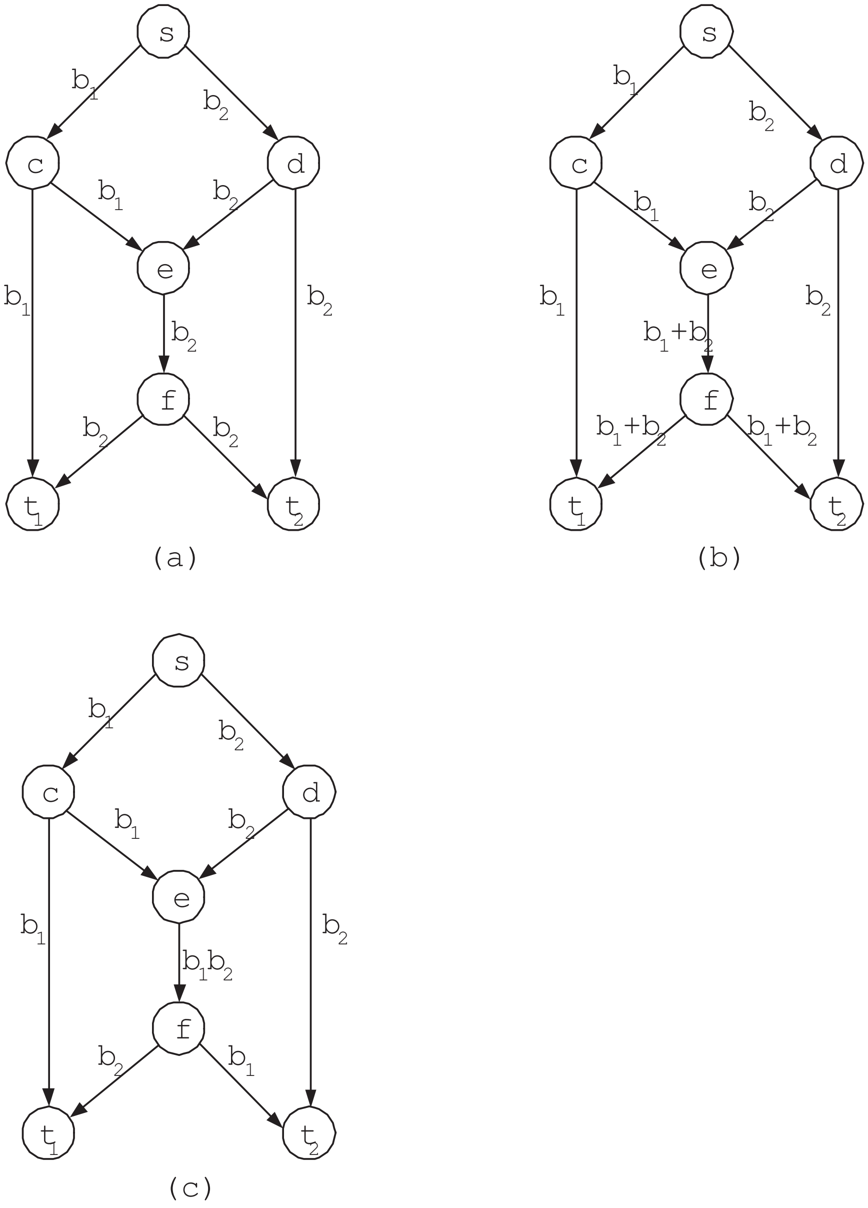
In existing computer networks, information is transmitted from the source node to each destination node through a chain of intermediate nodes by a method known as store-and-forward. In this method, data packets received from an input link of an intermediate node are stored and a copy is forwarded to the next node via an output link. In the case when an intermediate node is on the transmission paths toward multiple destinations, it sends one copy of the data packets onto each output link that leads to at least one of the destinations.

The fundamental concept of network coding was first introduced recently for communication networks in [3] and then fully developed in [1]. It is in [1] that the term ”‘network coding”’ was first introduced and the advantage of network coding over store-and-forward was first demonstrated.

There are various ways, each with different levels of generality, in formulating network code. Generally, a source node generates a pipeline of messages to be multicast to certain destinations. When the communication network is acyclic, operation at all the nodes can be so synchronized that each message is individually encoded and propagated from the upstream nodes to the downstream nodes. That is the processing of each message is independent of the sequential messages in the pipeline. In this way, the network coding problem is independent of the propagation delay, which includes the transmission delay over the channels as well as processing delay at the nodes. In this work, we mainly deal with acyclic networks.

On the other hand, when a network contains cycles, the propagation and encoding of sequential messages could convolve together. Thus the amount of delay becomes part of the consideration in network coding. The idea of convolutional network coding is first introduced in in [2,4]. The problems of convolutional network coding are more fully investigated later on in [43–46].

To illustrate the usefulness of network coding, let's first take a look at an example as denoted in Figure 1.1. The network in the figure has two sink nodes. It is easy to see that the maximum flow between s and t_1 or between s and t_2 are both equal to 2. So the maximum rate at which information at be sent from s to both t_1 and t_2 cannot be more than 2 bits. In Figure 1.1(a), we try to devise a routing scheme which sends 2 bits b_1 and b_2 to both t_1 and t_2. By symmetry, we send one bit on each output channel at node s. In this case, b_1 is sent on edge (s, c) and b_2 is sent on edge (s, d). At node c, b_1 is replicated and the copy is sent on the output channel. Similarly, at node d, b_2 is replicated and the copy is sent on the output channel. At node e, since both b_1 and b_2 are received but there is only one output channel, we have to choose one of the two bits to send on the output edge (e, f). Suppose we choose b_1 as in Figure 1.1(a). Then the bit is replicated at node f and the copies



(a)

(b)

(c)

Figure 1.1: a two sinks multi-source network

are sent to nodes t_1 and t_2. At node t_2, both b_1 and b_2 are received. However, at node t_1, two copies of b_1 are received but b_2 cannot be recovered. Thus this routing scheme does not work. Similarly, if b_2 instead of b_1 is sent on channel (e, f), b_1 cannot be recovered at node t_2. Therefore, we conclude that for this network, the max-flow bound cannot be achieved by routing and replication of bits.

However, if coding is allowed at the nodes, it is actually possible to achieve the max-flow bound. Figure 1.1(b) shows a scheme which sends 2 bits b_1 and b_2 to both nodes t_1 and t_2 where $'+'$ denotes modulo 2 addition. At node t_1, b_1 is received, and b_2 can be recovered by adding b_1 and $b_1 + b_2$, because

$$b_2 = b_1 + (b_1 + b_2). \tag{1.1}$$

Similarly, b_2 is received at node t_2, and b_1 can be recovered by adding b_2 and $b_1 + b_2$. Therefore, the max-flow bound is achieved. In this scheme, b_1 and b_2 are encoded into the codeword $b_1 + b_2$ which is then sent on channel ef. If coding at a node is not allowed, in order to send both b_1 and b_2 to node t_1 and t_2, at least one more bit has to be sent. Figure 1.1(c) shows such a scheme. In this scheme, however, the capacity of channel (e, f) is exceeded by 1 bit.

Next, we are going to give a formal definition of a network code.

1.1 Network Code

A communication network is a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ allowing multiple edges from one node to another where $\mathcal{V}$ is the set of nodes in $\mathcal{G}$ and $\mathcal{E}$ is the set of edges in $\mathcal{G}$. Every edge in the graph represents a communication channel with the capacity (in the sense of graph theory, e.g., [42]) of one data unit per unit time. A node without any incoming edge is a source node of the network. There exists at least one source node on every acyclic network. Throughout the text, a lower-case letter s will be used to represent the source node when there is just one source node within the network being discussed.

For every node $a \in \mathcal{V}$, let $In(a)$ denote the set of incoming channels to a and $Out(a)$ the set of outgoing channels from a. Meanwhile, let $In(s)$ denote a set of imaginary channels, which terminate at the source node s but are without originating nodes. The number of these imaginary channels is context dependent and always denoted by n. A data unit is represented by an element of a certain base field $\mathbb{F}$. For example, $\mathbb{F} = GF(2)$ when the data unit is a bit. A message consists of n data units and is therefore represented by an n-dimensional row vector $\mathbf{x} \in \mathbb{F}^n$. The source node s generates a message $\mathbf{x}$ and sends it out by transmitting a symbol over every outgoing channel. Message propagation through the network is achieved by the transmission of a symbol $\widetilde{f}_e(\mathbf{x}) \in \mathbb{F}$ over every channel $e \in \mathcal{E}$ in the network.

A non-source node a may not be able to identify and recover the value of the source message $\mathbf{x}$. For each channel e in $Out(a)$, node a simply encode all the received symbols from all the channels in $In(a)$ to a symbol $\widetilde{f}_e(\mathbf{x})$ which is then transmitted on e. A network code is specified by such an encoding mechanism for every channel.

Definition 1.1 (Local description of a network code on an acyclic network)**.** *Let $\mathbb{F}$ be a finite field and n a positive integer. An n-dimensional $\mathbb{F}$-valued network code on an acyclic communication network consists* *of a local encoding mapping*

$$\widetilde{k}_e : \mathbb{F}^{|In(a)|} \longrightarrow \mathbb{F} \tag{1.2}$$

for each node a in the network and each channel $e \in Out(a)$.

Due to the acyclic nature of the network, we can assume an order on $\mathcal{E}$ which is consistent with the associated partial order on $\mathcal{G}$. The acyclic topology of the network provides an upstream-to-downstream procedure for the local encoding mappings to accrue into the values $\widetilde{f}_e(\mathbf{x})$ transmitted over all channel e. The above definition of a network code does not explicitly give the value of $\widetilde{f}_e(\mathbf{x})$. Therefore, an equivalent definition will be presented below, which describes a network code by both the local encoding mechanisms as well as the recursively derived values $\widetilde{f}_e(\mathbf{x})$.

Definition 1.2 (Global description of a network code on an acyclic network)**.** *Let $\mathbb{F}$ be a finite field and n a positive integer. An n-dimensional $\mathbb{F}$-valued network code on an acyclic communication network consists of a local encoding mapping $\widetilde{k}_e : \mathbb{F}^{|In(a)|} \longrightarrow \mathbb{F}$ and a global encoding mapping $\widetilde{f}_e : \mathbb{F}^n \longrightarrow \mathbb{F}$ for each channel e in the network such that:*

1. *For every node a and every channel $e \in Out(a)$, $\widetilde{f}_e(\mathbf{x})$ is uniquely determined by $(\widetilde{f}_d(\mathbf{x}), d \in In(a))$, and $\widetilde{k}_e$ is the mapping via*

$$(\widetilde{f}_d(\mathbf{x}), d \in In(a)) \mapsto \widetilde{f}_e(\mathbf{x}). \tag{1.3}$$

2. *For the n imaginary channels e, the mappings $\widetilde{f}_e$ are the projections from the space $\mathbb{F}^n$ to the n different coordinates, respectively.*

Network codes that involved only linear mappings are of particular interest. The main reason is that network codes are in generally difficult to construct and with high implementation complexity. In order to allow the network code to be simple enough to be constructed, we try to confine our interest to network coding composes of linear operations only.

When a global encoding mapping $\widetilde{f}_e$ is linear, it corresponds to an n-dimensional column vector f_e such that $\widetilde{f}_e(\mathbf{x})$ is the product $\mathbf{x} \cdot f_e$, where the n-dimensional row vector $\mathbf{x}$ represents the message generated by s. Similarly, when a local encoding mapping $\widetilde{k}_e$, where $e \in Out(a)$, is linear, it corresponds to an $|In(a)|$-dimensional column vector k_e such that $\widetilde{k}_e(y) = y \cdot k_e$, where $y \in F^{|In(a)|}$ is the row vector representing the symbols received at the node a. In an n-dimensional $\mathbb{F}$-valued network code on an acyclic communication network, if all the local encoding mappings are linear, then so are the global encoding mappings since they are functional compositions of the local encoding mappings. The converse is also true. If the global encoding mappings are all linear, then so are the local encoding mappings.

Let a pair of channels (e_i, e_j) be called an adjacent pair when there exists a node a with $e_i \in In(a)$ and $e_j \in Out(a)$. Below, a linear network code is formulated as a network code where all the local and global encoding mappings are linear. Again, both the local and global descriptions are presented even though they are equivalent.

Definition 1.3 (local description of a linear network code on an acyclic network)**.** *Let $\mathbb{F}$ be a finite field and n a positive integer. An n-dimensional $\mathbb{F}$-valued linear network code on an acyclic communication network con-*

sists of a scalar k_{e_i,e_j}, called the local encoding kernel, for every adjacent pair (e_i, e_j). Meanwhile, the local encoding kernel at the node a means the $|In(a)| \times |Out(a)|$ matrix $K_a = [k_{e_i,e_j}]_{e_i \in In(a), e_j \in Out(a)}$.

Definition 1.4 (global description of a linear network code on an acyclic network)**.** *Let $\mathbb{F}$ be a finite field and n a positive integer. An n-dimensional $\mathbb{F}$-valued linear network code on an acyclic communication network consists of a scalar k_{e_i,e_j} for every adjacent pair (e_i, e_j) in the network as well as an n-dimensional column vector f_{e_j} for every channel e_j such that:*

1. $f_{e_j} = \sum_{e_i \in In(a)} k_{e_i,e_j} f_{e_i}$, *where* $e_j \in Out(a)$.
2. *The vectors f_{e_j} for the n imaginary channels $e_i \in In(s)$ form the natural basis of the vector space $\mathbb{F}^n$.*

The vector f_e is called the global encoding kernel for the channel e.

1.2 Properties of a Linear Network Code

In this section, we will give out the definition of various kinds of linear network code that are most commonly discussed in the literature, namely, linear multicast, linear broadcast, linear dispersion and generic linear network code. In addition, every one of them have been shown to be existed if the size of the field $\mathbb{F}$ that linear code are constructed upon is large enough.

With any coding schemes, the data flow at any intermediate node need to obey the law of information conservation. That is, the content of information sent out from any group of non-source nodes must be derived from the accumulated information received by the group from outside. In particular, the content of any information coming out of a non-source node must be derived from the accumulated information received by that node. Denote the maximum flow from s to a non-source node t as $maxflow(t)$. From the Max-flow Min-cut Theorem [28, 29], the information rate received by the node t obviously cannot exceed $maxflow(t)$. Similarly, denote the maximum flow from s to a collection $\wp$ of non-source nodes as $maxflow(\wp)$. Then, the information rate from the source node to the collection $\wp$ cannot exceed $maxflow(\wp)$.

Whether this upper bound is achievable depends on the network topology, the dimension n, and the coding scheme. Three special classes of linear network codes are defined below by the achievement of this bound to three extends. The conventional notation $\langle\cdot\rangle$ for the linear span of a set of vectors will be employed.

Definition 1.5. *Let vectors f_e denote the global encoding kernels in an n-dimensional $\mathbb{F}$-valued linear network code on an acyclic network. Write $V_t = \langle\{f_e : e \in In(t)\}\rangle$. Then, the linear network code qualifies as a linear multicast, a linear broadcast, or a linear dispersion, respectively, if the following statements hold:*

1. *$dim(V_t) = n$ for every non-source node t with $maxflow(t) \geq n$.*
2. *$dim(V_t) = min\{n, maxflow(t)\}$ for every non-source node t.*
3. *$dim\left(\langle\cup_{t\in\wp} V_t\rangle\right) = min\{n, maxflow(\wp)\}$ for every collection $\wp$ of non-source nodes.*

From the definitions, we can easily see that every linear dispersion is a linear broadcast, and every linear broadcast is a linear multicast.

However, the converse is not necessarily true. From the above definitions, we can see that the problem of whether a certain linear code exists or not depends mainly on the number of linearly independent global encoding kernels that the sink nodes can receive. Therefore, one way to construct a linear multicast/broadcast/dispersion is by considering a linear network code in which every collection of global encoding kernels that can possibly be linearly independent is linearly independent. This motivates the following concept of a generic linear network code.

Definition 1.6. *Let $\mathbb{F}$ be a finite field and n a positive integer. An n-dimensional $\mathbb{F}$-valued linear network code on an acyclic communication network is said to be generic if:*

- *Let $\{e_1, e_2, ..., e_m\}$ be an arbitrary set of channels, where each $e_j \in Out(a_j)$. Then, the vectors $f_{e_1}, f_{e_2}, ..., f_{e_m}$ are linearly independent (and hence $m \leq n$) provided that*

$$\langle\{f_e : e \in In(a_j)\}\rangle \not\subset \langle\{f_{e_k} : k \neq j\}\rangle \, \textit{for} \; 1 \leq j \leq m. \tag{1.4}$$

Generic network code has been proved to exist when the base field $\mathbb{F}$ is sufficiently large. Every generic network is in fact, on the other hand, a linear dispersion. Thus, a generic network code, a linear dispersion, a linear broadcast, and a linear multicast are notions of decreasing strength in this order with regard to linear independence among the global encoding kernels. The existence of a generic linear network code then implies the existence of the rest.

Theorem 1.1. *([10]) Given a positive integer n and an acyclic network, there exists an n-dimensional $\mathbb{F}$-valued generic linear network code for sufficiently large base field $\mathbb{F}$.*

Corollary 1.1. *([10]) Given a positive integer n and an acyclic network, there exists an n-dimensional $\mathbb{F}$-valued generic linear dispersion for sufficiently large base field $\mathbb{F}$.*

Corollary 1.2. *([10]) Given a positive integer n and an acyclic network, there exists an n-dimensional $\mathbb{F}$-valued generic linear broadcast for sufficiently large base field $\mathbb{F}$.*

Corollary 1.3. *([10]) Given a positive integer n and an acyclic network, there exists an n-dimensional $\mathbb{F}$-valued generic linear multicast for sufficiently large base field $\mathbb{F}$.*

1.3 Historical note

It was first shown by Ahlswede et al. [1] that the network capacity for network multicast satisfies the max-flow min-cut theorem, and this capacity can be achieved by network coding. Li, Yeung, and Cai [2] further showed that it is sufficient to consider linear network codes only. Subsequently, Koetther and Médard [4] developed a matrix framework for network coding. Jaggi et al. [11] proposed a deterministic polynomial-time algorithm to construct network codes. Ho et al. [26] showed that linear network codes can be effectively constructed by a randomized algorithm with an exponentially decreasing probability of error. Researchers have extended the above results to a variety of areas including wireless networks [32–34], energy [35], secrecy [5], error-correcting [18], content distribution [36], and distributed storage [37].

□ **End of chapter.**

Chapter 2

Secure Network Code

Summary

In the paradigm of network coding, the nodes in a network are allowed to encode the information received from the input links. With network coding, the full capacity of the network can be utilized. In this chapter, we discuss the model proposed by Cai and Yeung [5] which incorporates network coding and information security.

Most of the studies in the literature of network coding assume that the network is secure, or eavesdropper-free. Cai and Yeung [5] introduce the idea secure network coding which can be used to handle the secure problem of network coding transmission in the presence of an adversary in the network.

In this chapter, we are going to study a model of secure network code in which a collection of subsets of the channels in the network is given, and an eavesdropper is allowed to access any one (but not more than one) of these subsets without being able to obtain any information about the message transmitted. The model includes secret sharing in classical cryptography as a special case. Cai and Yeung have proved in [5] that there exists a construction of secure linear network codes provided that a certain graph-theoretic sufficient condition is satisfied. The proof for the necessity of this condition for the special case that the eavesdropper may choose to access any subset of channels of a fixed size is also given in [13].

The work by Cai and Yeung [5] can be considered as a network generalization of the idea that a sender has to randomize the message to be transmitted in order to protect it from the eavesdropper. Suppose a sender wants to send the output of a random message M with alphabet $\mathcal{M} = \{0, 1, \ldots p - 1\}$ to a receiver. The sender can send information via a "public" channel, whose output can be accessed by the receiver as well as an eavesdropper who tries to obtain some information about M, or the sender can send information via a "secure" channel, whose output can be accessed only by the receiver. The usual way to protect M from the eavesdropper is that the sender generates a "secret key" K independent of the source M according to the uniform distribution over $\mathcal{M}$. Let x be the outcome of M, and let r be the outcome of K. Then the sender sends the key r to the receiver via the secure channel, and sends $x+r \pmod p$ via the public channel. Upon receiving both r and $x + r$, the receiver as the legal user can recover x because $x = (x + r) - r$. On the other hand, the wiretapper cannot obtain any information about m by knowing $x + r$ alone because what he/she knows is a total randomization of the message x.

The main idea in the above scheme is that the sender has to randomize the message in order to protect it from the wiretapper, where in this case the alphabet sets of the random key and of the information source have the same size (the two alphabet sets are the same). Shannon showed in [30] that this protocol is optimal in the sense of minimizing the size of the random key. This result, known as the perfect secrecy theorem, has been generalized to the imperfect secrecy theorem by Yeung [31] (p. 116).

2.1 Communication System on a Wiretap Network

First, we will present a model of a communication system on a wiretap network (CSWN) [5], which subsumes the secret-sharing model proposed independently by Blakley [14] and Shamir [15]. Then we will define a code for a CSWN.

A CSWN consists of the following components:

i) *Directed multigraph* $\mathcal{G}$: The pair $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ is called a directed multigraph, where $\mathcal{V}$ and $\mathcal{E}$ are the node set and the edge set of $\mathcal{G}$, respectively. In our model, we assume that $\mathcal{G}$ is acyclic, that is, it does not contain a directed cycle.

ii) *Source node* s: The node set $\mathcal{E}$ contains a node s, called the source node, where a random message M taking values in an alphabet $\mathcal{M}$ is generated.

iii) *Set of user nodes* $\mathcal{T}$: A user node is a node in $\mathcal{V}$ which is fully accessed by a legal user who is required to receive the random message M with zero error. There is generally more than one user node in a network. The set of user nodes is denoted by $\mathcal{T}$.

iv) *Collection of sets of wiretap edges* $\mathcal{W}$: $\mathcal{W}$ is a collection of subsets of the edge set $\mathcal{E}$. Each member of $\mathcal{W}$ may be fully accessed by a eavesdropper, but no eavesdropper may access more than one member of $\mathcal{W}$.

The eavesdropper is assumed to be able to gain access to any one, but not more than one, member of $\mathcal{W}$. And we further assume that no one but the eavesdropper will know which set of channels are eavesdropped.

The quadruple $(\mathcal{G}, s, \mathcal{T}, \mathcal{W})$ is referred as a CSWN. The multigraph $\mathcal{G}$ is referred as a network and the edges in $\mathcal{E}$ are referred as channels. The random message M is generated at the source node s according to the uniform distribution on an alphabet set $\mathcal{M}$. On each channel in $\mathcal{E}$, an index taken from an alphabet set $\mathbb{F}$ can be transmitted.

One interesting question would be the maximum rate at which information can be multicast to the sink nodes under the presence of such an eavesdropper. In this chapter, we will discuss maximum value of $|\mathcal{M}|$ for which the message M can be multicast from the source node s to the set of user nodes $\mathcal{T}$, while the message M is protected from eavesdropper who can access any set of channels in $\mathcal{W}$.

It worth noting that in the CSWN model, if eavesdropper is absent, that is, $\mathcal{W} = \emptyset$, a CSWN is reduced to the model studied in [1] and [2]. It was proved in [1] that information can be multicast from the source node s to all the user nodes in $\mathcal{T}$ at rate n if and only if the value of a maximum flow from s to each user node is at least n in the graph $\mathcal{G}$. In general, information can be multicast from the source node to the user nodes at a higher rate with network coding than the traditional "store and forward" routing scheme when there are at least two user nodes. Subsequently, it was proved in [2] by an explicit construction that this can be achieved by linear network codes. Based on this result, it would be interesting know what is the maximum rate at which information can be multicast in the presence of an eavesdropper and how to construct a linear network code that can obtain such a maximum data rate.

To protect the message from being eavesdropped, it can be easily shown that randomizing the message is a necessary measure. If there is no randomness in the network, the index transmitted on any channel is a function of the message M and hence is not independent of M unless the index takes a constant value. If this is the case, the channel becomes degenerate as it cannot transmit any useful information through.

Let K be an random variable, independent of the message M, that takes values in an alphabet set $\mathcal{K}$ according to the uniform distribution. A code for a CSWN consists of a set of local encoding mappings $\widetilde{f_e} : e \in \mathcal{E}$ such that for all e, $\widetilde{f_e}$ is a function from $\mathcal{M} \times \mathcal{K}$ to $\mathbb{F}$ if $e \in Out(s)$, and is a function from $\mathbb{F}^{|In(a)|}$ to $\mathbb{F}$ if $e \in Out(a)$ for $a \neq s$. For $e \in \mathcal{E}$, let Y_e be the random symbol in $\mathbb{F}$ transmitted on channel e, i.e., the value of $\widetilde{f_e}$. For a subset B of $\mathcal{E}$, denote $(Y_e : e \in B)$ by Y_B.

To complete the description of a code, we have to specify the order in which the channels send the indices. Since the graph $\mathcal{G}$ is acyclic, it defines a partial order on the node set $\mathcal{E}$. Then the nodes in $\mathcal{V}$ can be indexed in a way such that for two nodes a and a' , if there is a channel from node a to node a' , then $a < a'$. According to this indexing, node a sends symbols in its output channels before node a' if and only if $a < a'$. The order in which the channels within the set of output channels of a node sends the symbols is immaterial. The important point here is that whenever a channel sends a symbol, all the symbols necessary for encoding have already been received. A code defined as such induces a function Φ_t from $\mathcal{M} \times \mathcal{K}$ to $\mathbb{F}^{|In(t)|}$ for all user nodes $t \in \mathcal{T}$, where the value of Φ_t denotes the symbols received by the user node t in its input channels.

A code $\widetilde{f}_e : e \in \mathcal{E}$ is admissible for a CSWN $(\mathcal{G}, s, \mathcal{T}, \mathcal{W})$ if the following conditions are satisfied:

i) For all user nodes $t \in \mathcal{T}$ and all $\mathbf{m}, \mathbf{m}' \in \mathcal{M}$ with $\mathbf{m} \neq \mathbf{m}'$,

$$\Phi_t(\mathbf{m}, \mathbf{k}) \neq \Phi_t(\mathbf{m}', \mathbf{k}') \tag{2.1}$$

for all $\mathbf{k}, \mathbf{k}' \in \mathcal{K}$. This guarantees that any two messages are distinguishable at every user node, and we refer to this as the decodable condition.

ii) For all $\mathrm{W} \in \mathcal{W}$

$$H(M|Y_{\mathrm{W}}) = H(M). \tag{2.2}$$

Here $H(\cdot|\cdot)$ and $H(\cdot)$ denote conditional entropy and entropy, respectively. In other words, M and Y_{W} are independent. This is referred to as the security condition.

2.2 Construction of Admissible Codes

Cai and Yeung [13] defined a class of linear codes for a CSWN by the following construction.

Construction 1

i) Choose suitable positive integers n and r, where $r < n$. The random message M is distributed uniformly on $GF^{(n-r)}(q)$, while the independent random key K is distributed uniformly on $GF^r(q)$. Let the outcome $\mathbf{m}$ of M be a row vector in $GF^{(n-r)}(q)$ and the outcome $\mathbf{k}$ of K be a row vector in $GF^r(q)$. Let $\mathbf{x} = (\mathbf{m}, \mathbf{k})$.

ii) Choose a suitable n-dimensional linear network code on $\mathcal{G}$.

iii) Encode the vector $\mathbf{x}$ by transmitting in each channel e the value $\mathbf{x}f_e$.

Cai and Yeung [13] have also shown that by choosing n, r and the linear network code probably, the code can be made to be admissible, i.e., decodable and secure.

Theorem 2.1. *([5]) There exists an admissible code on $\mathcal{G}$ over $GF(q)$ for $q > |\mathcal{W}|$ by Construction 1 if there exists an n-dimensional linear network code over $GF(q)$ such that for all user nodes $t \in \mathcal{T}$,*

$$dim(V_t) = n, \tag{2.3}$$

and for all wiretap sets of channels $W \in \mathcal{W}$,

$$dim(V_W) \leq r. \tag{2.4}$$

In the directed graph $\mathcal{G}$, a path is a sequence of channels $e_1, e_2, \ldots, e_l$ such that for $1 \leq i \leq l-1$, there exists $t_i \in \mathcal{V}$ such that $e_i \in In(t_i)$ and $e_{i+1} \in Out(t_i)$. Two paths are disjoint if they do not share a common channel (but they may share a common node). The following theorem is similar to Theorem 2.1, but the condition therein depends only on the graph $\mathcal{G}$ and the collection of wiretap channels $\mathcal{W}$.

Theorem 2.2. *([5]) Let $\mathcal{G}^* = (\mathcal{V}, \mathcal{E}^*)$, where $\mathcal{E}^* \subset \mathcal{E}$, be a subgraph of $\mathcal{G}$ satisfying the following:*

i) For any $t \in \mathcal{T}$, there are n disjoint paths in $\mathcal{G}^*$ from the source node s to the user node t.

ii) For any $W \in \mathcal{W}$, there are at most r disjoint paths in $\mathcal{E}^*$ from the source node s to the channels in $W \subset \mathcal{E}^*$.

If such a subgraph $\mathcal{G}^*$ exists, then there exists an admissible linear network code on $\mathcal{G}$ over $GF(q)$ by Construction 1 for $q > max\{|\mathcal{T}|, |\mathcal{W}|\}$.

It has also been shown in [13] that the conditions in Theorem 2.2 is also a necessary condition for a special case in which the eavesdropper may choose to access any subset of channels of a fixed size r. As a whole, it has been shown that in the presence of an eavesdropper which can eavesdrop a randomly chosen and fixed set of r channels in the network, the general maximum rate at which information can be multicast from the source node and the user nodes is equal to $n - r$. It has also been shown in [5] that in order to prevent the eavesdropper from obtaining any useful information about $\mathbf{x}$ in the special being discussed, at least r units of randomness need to be injected into the network.

2.3 Historical note

The problem of secure network coding was first studied by Cai and Yeung in [5]. They introduced the CSWN, which subsumes the secret-sharing model proposed independently by Blakley [14] and Shamir [15], and proposed a secure network coding scheme. Such secure network codes have been further studied in [12] by Feldman et. al. Later on, Cai and Yeung continued their original work in [6] with a more general model in which there are more than one source node and randomness can be generated at an arbitrarily given subset of nodes, and obtained a necessary and sufficient condition for the security of a network code. In their latest work [13], they further provide the code that can achieve the required security while using the minimum amount of randomness and multicasting maximum possible amount of information for the special case that the eavesdropper may choose to access any subset of channels of a fixed size.

□ **End of chapter.**

Chapter 3

Error-correcting Network Code

Summary

In this chapter, the weight properties of linear network codes are investigated. Some new weight definitions, called the network Hamming weight, for error vectors, received vectors and message vectors will be introduced. All these network Hamming weights reduce to the usual Hamming weight in the special case of classical error correction. With these network Hamming weights, the minimum distance of a network code can be defined. This aim of this chapter is to review on the existing work in characterizing the ability of network codes for error correction, error detection and erasure correction in terms of the minimum distances of the codes.

Transmission over networks is assumed to be error-free [10] in most of the works in the literature. In practical, however, transmission may suffer from different kinds of errors, such as random errors, link failures, traffic congestion and malicious modifications. In some previous study, researchers have already noticed that network coding can be used to detect and correct errors in networks [16–21].

The concept of error-correcting network coding, a generalization of classical error correction coding, was first introduced by Cai and Yeung [18–20]. They generalized the Hamming bound, the Singleton bound and the Gilbert-Varshamov bound in classical error correction coding to network coding. The Hamming bound, the Singleton bound, and the Gibert- Varshamov bound are fundamental bounds in classical algebraic coding theory [38–41]. Zhang [21] introduced the minimum rank for linear network codes, which plays a role similar to that of the minimum distance in decoding classical error-correcting codes. The relation between network coding and classical algebraic coding has been clarified in [10].

In this chapter, we study the problem of error-correcting network code which will lead to the following properties of linear network code assembling resembling those of the classical algebraic error-correcting code. Let d be an integer. The following properties of a linear network code can be shown to be equivalent:

i) The multicast minimum distance of the code is larger than or equal to $d + 1$.

ii) The code can correct all error vectors with Hamming weight less than $(d + 1)/2$.

iii) The code can detect all non-zero error vectors with Hamming weight less than or equal to d.

iv) The code can correct all erasures will Hamming weight less than or equal to d.

3.1 Problem Formulation

A multicast on $\mathcal{G}$ transmits information from a source node s to a set of sink nodes $\mathcal{T}$. Let $n_s = |Out(s)|$. The source node s modulates the information to be multicast into a row vector $\mathbf{x} \in \mathbb{F}_q^{n_s}$ called the message vector. The vector is sent in one use of the network by mapping the n_s components of the vector onto each edges in $Out(s)$. Define an $n_s \times |\mathcal{E}|$ matrix $A = [A_{i,j}]$ as

$$A_{i,j} = \begin{cases} 1 & e_j \text{ is the } ith \text{ edge in } Out(s), \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

By applying the order on $\mathcal{E}$ to $Out(s)$, the n_s nonzero columns of A form an identity matrix. An error vector $\mathbf{z}$ is an $|\mathcal{E}|$-tuple with each component representing the error on an edge.

A network code for network $\mathcal{G}$ is specified by a set of local encoding functions $k_{e_i,e_j} : e_i, e_j \in \mathcal{E}$ and the message set $\mathcal{C}$. Define the $|\mathcal{E}| \times |\mathcal{E}|$ one-step transition matrix $K = [K_{i,j}]$ for network $\mathcal{G}$ as

$$K_{i,j} = \begin{cases} k_{e_i,e_j} & e_i \in In(a), e_j \in Out(a) \text{ for some } a \in \mathcal{V}, \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

For an acyclic network, $K^N = 0$ for some positive integer N. Define the transfer matrix of the network by $F = (I - K)^{-1}$ [4], so that the symbols transmitted on the edges are given by the components of

$(\mathbf{x}A + \mathbf{z})F$.

For a sink node $t \in \mathcal{T}$, write $n_t = In(t)$, and define an $|\mathcal{E}| \times n_t$ matrix $B_t = [B_{i,j}]$ for sink node t as

$$B_{i,j} = \begin{cases} 1 & e_i \text{ is the } jth \text{ edge in } In(t), \\ 0 & \text{otherwise.} \end{cases} \tag{3.3}$$

The n_t nonzero rows of B_t form a permutation matrix. The received vector for a sink node t is

$$y_t = (\mathbf{x}A + \mathbf{z})FB_t \tag{3.4}$$

$$= \mathbf{x}F_{s,t} + \mathbf{z}F_t, \tag{3.5}$$

where $F_{s,t} = AFB_t$ is the transfer matrix induced by the linear network code, A is an $|Out(s)| \times |\mathcal{E}|$ matrix that choose the rows vectors of F corresponding to the outgoing edges from s, and B_t is an $|\mathcal{E}| \times |In(t)|$ matrix which choose the column vectors of F corresponding to the incoming edges of the sink node t.

Equation (3.5) is the formulation of the multicast network error correction problem. The classical error correction problem is a special case in which both of $F_{s,t}$ and F_t reduce to identity matrices. The message transmission capacity is measured by the rank of the transfer matrix $F_{s,t}$. Denote the maximum flow between source node s and sink node t by $maxflow(s,t)$. Evidently, for any linear network code on $\mathcal{G}$, the rank of $F_{s,t}$ is upper bounded by $maxflow(s,t)$ [10]. Let $\mathcal{C}$ be the set of message vectors that can be transmitted by the source and be decoded correctly. When the network is error-free, the error correction problem is reduced to the usual network coding problem, for which the size of

$\mathcal{C}$ is upper bounded by $q^{min_{t\in\mathcal{T}} maxflow(s,t)}$ [1].

3.2 Network Hamming Weight and Error-correction

Next, weights and distances for network codes defined in [22] will be introduced.

For any $t \in \mathcal{T}$, let $\Upsilon_t(\mathbf{y}) = \{\mathbf{z} : \mathbf{z}F_t = \mathbf{y}\}$ for a received vector $\mathbf{y} \in Im(F_t)$, the image space of F_t.

Definition 3.1. *For any sink t, the network Hamming weight of a received vector $\mathbf{y}$ is defined by*

$$W_t^{rec}(\mathbf{y}) = \min_{\mathbf{z}\in\Upsilon_t(\mathbf{y})} w_H(\mathbf{z}). \tag{3.6}$$

Definition 3.2. *For any sink t, the network Hamming weight of an error vector $\mathbf{z}$ is defined by*

$$W_t^{err}(\mathbf{z}) = W_t^{rec}(\mathbf{z}F_t). \tag{3.7}$$

In other words, $W_t^{err}(\mathbf{z})$ is the minimum Hamming weight of any error vector that causes the same confusion at sink t as the error vector $\mathbf{z}$. For any vector $\mathbf{z} \in \Upsilon_t(\mathbf{0})$, $W_t^{err}(\mathbf{z}) = W_t^{rec}(\mathbf{0}) = \min_{z\in\Upsilon_t(\mathbf{0})} w_H(\mathbf{z}) = w_H(\mathbf{0}) = 0$. If error vectors $\mathbf{z}_1$ and $\mathbf{z}_2$ satisfy $\mathbf{z}_1 - \mathbf{z}_2 \in \Upsilon_t(\mathbf{0})$, then $W_t^{err}(\mathbf{z}_1) = W_t^{rec}(\mathbf{z}_1F_t) = W_t^{rec}(\mathbf{z}_2F_t) = W_t^{err}(\mathbf{z}_2)$. Thus Definition 3.2 satisfies the two conditions required for the definition of the weight of error vectors:

i) If $\mathbf{z}F_t = \mathbf{0}$, then the weight of $\mathbf{z}$ is zero;

ii) If the difference of two error vectors is an error vector with weight $\mathbf{0}$, then these two error vectors have the same weight.

Definition 3.3. *For any sink t, the network Hamming weight of a message vector $\mathbf{x}$ is defined by*

$$W_t^{msg}(\mathbf{x}) = W_t^{rec}(\mathbf{x}F_{s,t}). \tag{3.8}$$

In other words, $W_t^{msg}(\mathbf{x})$ is the minimum Hamming weight of any error vector that has the same effect on sink t (when the message vector is $\mathbf{0}$) as the message vector $\mathbf{x}$ (when the error vector is $\mathbf{0}$).

Definition 3.4. *For any $t \in \mathcal{T}$, the network Hamming distance between two received vectors $\mathbf{y}_1$ and $\mathbf{y}_2$ is defined by*

$$D_t^{rec}(\mathbf{y}_1, \mathbf{y}_2) = W_t^{rec}(\mathbf{y}_1 - \mathbf{y}_2). \tag{3.9}$$

Definition 3.5. *For any $t \in \mathcal{T}$, the network Hamming distance between two message vectors $\mathbf{x}_1$ and $\mathbf{x}_2$ is defined by*

$$D_t^{msg}(\mathbf{x}_1, \mathbf{x}_2) = W_t^{msg}(\mathbf{x}_1 - \mathbf{x}_2). \tag{3.10}$$

When $F_t = F_{s,t} = I$, these definitions reduce to the usual Hamming weight and Hamming distance.

A message set $\mathcal{C}$ for a multicast in network $\mathcal{G}$ is a subset of the vector space F^{n_s}.

Definition 3.6. *The unicast minimum distance of a network code with message set $\mathcal{C}$ for sink node t is defined by*

$$d_{\min,t} = \min\{D_t^{msg}(\mathbf{x}, \mathbf{x}') : \mathbf{x}, \mathbf{x}' \in \mathcal{C}, \mathbf{x} \neq \mathbf{x}'\}.$$

Definition 3.7. *The multicast minimum distance of a network code with message set $\mathcal{C}$ is defined by*

$$d_{\min} = \min_{t \in \mathcal{T}} d_{\min,t}.$$

It has been shown that the following properties of a linear network code are equivalent:

Theorem 3.1. *([22]) The following properties of a network code are equivalent:*

1. *The code can correct any error vector $\mathbf{z}$ with $w_H(\mathbf{z}) \leq c$ at all the sink nodes.*
2. *The code can correct any error vector $\mathbf{z}$ with $W^{err}(\mathbf{z}) \leq c$ at all the sink nodes.*
3. *The code has $d_{min} \geq 2c + 1$.*

where c is a non-negative integer.

3.3 Network Erasure Correction

When a channel in the network fails, the channel generates no valid outputs, and we say that an erasure has occurred. If the local encoding function of a node depends on the output of that channel, the code has to assume that a default symbol in the finite field $\mathbb{F}$ is received on that channel when an erasure occurs. So associated with each channel is a default symbol. Here, we consider a network in which only erasures can occur in the channels, and the sink nodes know the set of channels on which erasures occur. However, we make no assumption that the default symbols of the channels are know by the sink nodes. In other words, we can simply assume that a random symbol will be transmitted in a channel if an erasure occurs in that channel. As before, we assume that sink node t knows the message set $\mathcal{C}$ as well as the transfer matrices $F_{s,t}$ and F_t.

Two quantities will be employed to characterize the ability of a network code for erasure correction. The first one is the Hamming weight of an erasure pattern ρ, denoted by $|\rho|$. The second one, called the network Hamming weight of an error pattern ρ, is defined as $W_t^{esr}(\rho) = \max_{\mathbf{z}\in\rho^*} W_t^{err}(\mathbf{z})$ where ρ^* is the set of erasure vectors that match ρ. Since $W_t^{esr}(\mathbf{z}) \leq w_H(\mathbf{z}) \leq |\rho|$ for any $\mathbf{z} \in \rho^*$, we have

$$W_t^{esr}(\rho) \leq |\rho|. \tag{3.11}$$

For an erasure pattern ρ, define the multicast weight as

$$W^{esr}(\rho) = \max_{t\in\mathcal{T}} W_t^{esr}(\rho).$$

It has been shown that the following properties of a linear network code are equivalent:

Theorem 3.2. *([22]) The following properties of a network code are equivalent:*

1. *The code can correct any erasure pattern ρ with $|\rho| \leq d$ at all the sink nodes.*

2. *The code can correct any erasure pattern ρ with $W^{esr}(\rho) \leq d$ at all the sink nodes.*

3. *The code has $d_{min} \geq d + 1$.*

where d is a non-negative integer.

3.4 Singleton Bound

In term of the notion of minimum distance, the Singleton bound obtained in [19] can be restated as

$$d_{min} \leq \min_{t \in \mathcal{T}} m_t - \omega + 1. \tag{3.12}$$

The tightness of (3.12) has been proved in [20]. In fact, it can readily be shown that for all $t \in \mathcal{T}$,

$$d_{min,t} \leq m_t - \omega + 1 \tag{3.13}$$

which is more refined than (3.12), specifically when m_t are not the same for all $t \in t$. And we have already shown that in [24] the tightness of (3.13) is achievable.

Theorem 3.3. *Given a set of local encoding kernels over a finite field with size q where q is sufficiently large, for every*

$$0 \leq \omega \leq \min_{t \in \mathcal{T}} m_t, \tag{3.14}$$

there exists a message set $\mathcal{C}$ with $|\mathcal{C}| = q^{\omega}$ such that

$$d_{\min,t} = m_t - \omega + 1 \tag{3.15}$$

for all sink nodes t.

Proof. See [24]. □

3.5 Historical note

The concept of error-correcting network coding, a generalization of classical error correction coding, was first introduced by Cai and Yeung [18–20]. They generalized the Hamming bound, the Singleton bound and the Gilbert-Varshamov bound in classical error correction coding to network coding. Zhang [21] introduced the minimum rank for linear network codes, which plays a role similar to that of the minimum distance in decoding classical error-correcting codes. The relation between network coding and classical algebraic coding has been clarified in [10].

□ **End of chapter.**

Chapter 4

Secure Error-Correcting (SEC) Network Codes

Summary

In this chapter, we propose a deterministic algorithm to construct secure error-correcting (SEC) network codes which can transmit information at rate $m-2d-k$ to all sink nodes, and prevent the information from eavesdropping and contamination during the transmission, where m is the minimum among the maxflows of all the sinks, d is the maximum network Hamming weight of the error vectors and k is the maximum cardinality of the subset of channels which can be eavesdropped. Such constructed network codes can also achieve the refined Singleton bound. Based on this algorithm we further present two transmission schemes which can achieve the transmission rate $m-d$, when the adversary satisfies an inaction assumption. We also show that in the presence of feedback, a rate beyond $m-d$ could be possibly achieved without reconstructing the existing network code.

In this chapter, we consider two kinds of adversaries at the same time:

i) Adversary that can contaminate the transmission on a subset of channels with cardinality less than or equal to d;

ii) Adversary that can eavesdrop another subset of channels with cardinality less than or equal to k.

Jaggi *et. al* [23] studied the similar problem using randomized design. Under the inaction assumption, where the adversary contaminates the same subset of channels for a long period of time, they presented a scheme which can achieve a rate $m - d$ asymptotically based on a secret channel, where m is the minimum among the maxflows of all the sink nodes. Their work considered that the adversary can make use of the eavesdropped information to contaminate the transmission. They proposed schemes that can prevent, with a high probability of success rate, the adversary from obtaining any useful information due to the randomized-nature of random network code.

The main contribution of this chapter is to propose a deterministic network code, called *secure error-correcting network codes* (SEC network codes), which can transmit information to all sink nodes at the rate of $m - 2d - k$ with complete reliability and completely free from eavesdropping by the adversary without the inaction assumption. The SEC network codes can also achieve the refined Singleton bound [24]. The SEC network codes give a practical realization of the secret channel. Based on the secret channel and under the inaction assumption, we present two deterministic schemes which can achieve the rate $m-d$. We also show that in the presence of feedback, a rate beyond $m - d$

could be achievable with the existing network code.

4.1 Combining Network error correction and secure network code

In this section, we give a constructive proof showing secure network coding and error-correcting network coding can in fact be carried out at the same time without affecting the capability of each other. Such network code is able to multicast information to sink nodes without revealing any information to the adversary and without suffering any unrecoverable data distortion under our assumption.

We first construct an error-correcting network code which can achieve the refined Singleton bound. After that, the error correcting network code will further be converted into a secure network code with capacity $m - 2d - k$ which can multicast information to all sink nodes securely as long as the number of channels that the adversary can listen to is less than or equal to k while maintaining its ability to correct at least d errors injected into the network by the adversary. It is worth noting that for any fixed choice of d error-correcting network code, the code can correct any d errors injected into the network. And it is possible for such a code to correct more than d errors if the dimension of the errors that are imposed by the the errors on all sink nodes is less than or equal to d.

By applying the result of Theorem 3.3, we can obtain a network code, with capacity $m - 2d$, such that

$$\begin{aligned} d_{min,t} =& m_t - (m - 2d) + 1 \qquad (4.1) \\ \geq& \, 2d + 1. \qquad (4.2) \end{aligned}$$

By the result of Theorem 3.1, such code can correct any error vector with hamming weight less than or equal to d.

4.1.1 Code Construction

In this subsection, we will present a code construction by cascading an error-correcting network code construction with a secure network code construction. The existence of such a code will also be shown while the error-correcting capability and the secure issue of the result network code will be analyzed in the next subsection.

For two subsets $V_1, V_2 \subset \mathbb{F}_q^{\omega+k}$, their sum is the set defined by

$$V_1 + V_2 = \{\mathbf{v}_1 + \mathbf{v}_2 : \mathbf{v}_1 \in V_1, \mathbf{v}_2 \in V_2\}. \qquad (4.3)$$

Denote by $\mathcal{W}$ a collection of subsets W of the edge set $\mathcal{E}$ such that $|W| \leq k$.

Construction 1:

i) By Theorem 3.3, we can construct a network code with message set $\mathcal{C}'$ where $|\mathcal{C}'| = q^{\omega+k}$, such that $d_{\min,t} = m_t - \omega - k + 1$ for all sink nodes t. Let G be the $(\omega + k) \times m$ generator matrix of $\mathcal{C}'$.

ii) For all $W \in \mathcal{W}$, define $\mathcal{L}_W = \langle\{Gf_e, e \in W\}\rangle$ where $\langle\cdot\rangle$ is the conventional notation for the linear span of a set of vectors. Then we choose ω linearly independent vectors $b_1, b_2, ..., b_\omega$ from $\mathbb{F}^{\omega+k}$

such that $\forall W \in \mathcal{W}$,

$$\langle \{b_1, b_2, ..., b_\omega\} \rangle \cap \mathcal{L}_W = \emptyset. \tag{4.4}$$

There existence of such a set of vectors will be justified later on. We can extend $b_1, b_2, ..., b_\omega$ to a linearly independent set with $\omega + k$ vectors, say $b_1, b_2, ..., b_\omega, b_{\omega+1}, ..., b_{\omega+k}$, and denote

$$Q = \begin{bmatrix} b_1 & b_2 & \dots & b_{\omega+k} \end{bmatrix}, \tag{4.5}$$

which is non-singular.

iii) The information source X takes values in $\mathbb{F}^\omega$ while the independent randomness R takes values in $\mathbb{F}^k$ according to the uniform distribution. Let the message $\mathbf{x}$ be a row vector in $\mathbb{F}^\omega$, and let the outcome $\mathbf{r}$ of R be a row vector in $\mathbb{F}^k$. Let $X' = (X, R)$ and the outcome of X' be $\mathbf{x}' = (\mathbf{x}, \mathbf{r})$.

iv) Encode the vector $\mathbf{x}'$ by $Q^{-1}G$ and transmit the encoded vector $\mathbf{x}'Q^{-1}G$ by utilizing the given network code. Therefore the information transmitting in each channel e is of the value $\mathbf{x}'Q^{-1}Gf_e$.

Justification of the existence of Q:

To prove the claim that there exist ω linearly independent vectors $b_1, b_2, ..., b_\omega$ from $\mathbb{F}^{\omega+k}$ such that $\forall W \in \mathcal{W}$,

$$\langle \{b_1, b_2, ..., b_\omega\} \rangle \cap \mathcal{L}_W = \emptyset. \tag{4.6}$$

We assume that we have already chosen $b_1, b_2, ..., b_{j-1}$ such that

$$\langle \{b_1, b_2, ..., b_{j-1}\} \rangle \cap \bigcup_{W \in \mathcal{W}} \mathcal{L}_W = \emptyset. \tag{4.7}$$

We can choose b_j as any vector not in $\langle\{b_1, b_2, ..., b_{j-1}\}\rangle + \bigcup_{W\in\mathcal{W}} \mathcal{L}_W$. To see the existence of such a b_j, we can observe that $\forall j, j \leq \omega$,

$$\begin{aligned}
&\left|\langle\{b_1, b_2, ..., b_{j-1}\}\rangle + \bigcup_{W\in\mathcal{W}} \mathcal{L}_W\right| && (4.8)\\
&\leq |\langle\{b_1, b_2, ..., b_{j-1}\}\rangle| \left|\bigcup_{W\in\mathcal{W}} \mathcal{L}_W\right| && (4.9)\\
&\leq |\mathbb{F}|^{j-1} \sum_{W\in\mathcal{W}} |\mathcal{L}_W| && (4.10)\\
&\leq |\mathbb{F}|^{j-1} \sum_{W\in\mathcal{W}} |\mathbb{F}|^k && (4.11)\\
&\leq |\mathbb{F}|^{j+k-1} |\mathcal{W}| && (4.12)\\
&\leq |\mathbb{F}|^{\omega+k-1} |\mathcal{W}| && (4.13)\\
&< |\mathbb{F}|^{\omega+k}, && (4.14)
\end{aligned}$$

when $|\mathbb{F}| > |\mathcal{W}|$.

By the facts that

i) $b_j \notin \langle\{b_1, b_2, ..., b_{j-1}\}\rangle + \bigcup_{W\in\mathcal{W}} \mathcal{L}_W$;

ii) $\langle\{b_1, b_2, ..., b_{j-1}\}\rangle \cap \bigcup_{W\in\mathcal{W}} \mathcal{L}_W = \emptyset$,

we can then infer that

$$\langle\{b_1, b_2, ..., b_j\}\rangle \cap \bigcup_{W\in\mathcal{W}} \mathcal{L}_W = \emptyset. \qquad (4.15)$$

4.1.2 Security and Error-correction ability of the Code Constructed

In this subsection, we are going to show that the code constructed in the previous subsection can correct up to d errors injected into the network and remain secure to the adversary that can eavesdrop any set of k channels in the network when information can be transmitted up to the rate of $m - 2d - k$.

Theorem 4.1. *Given a set of local encoding kernels over a finite field with size q where q is sufficiently large, there exists a message set $\mathcal{C}$ with $|\mathcal{C}| = q^{m-2d-k}$ such that information can be transmitted to all the sink nodes t at the rate $m - 2d - k$ in the presence of d channels with errors, and the network code can prevent eavesdroppings on any set of k channels in the network.*

Proof. By using construction 1, we can obtain a linear network code that allows us to transmit information at the rate ω. All we have to show now is that the code satisfies the error correcting condition and the security condition. We first verify the error correcting condition. By the result of Theorem 3.1, every sink node can decode and get back $\mathbf{x}'Q^{-1}$ in spite of any d errors injected, where $2d + 1 \leq \min_{t \in T} d_{min,t}$, errors injected into the network by the malicious party. Therefore, sink nodes can get back $\mathbf{x}'$ and hence $\mathbf{x}$ by multiplying the decoded information with Q.

Now, let us check the security condition. We first assume that no error is injected into the network. We first fix an arbitrary set W of $k' \leq k$ channels, $e_1, e_2, ..., e_{k'}$ such that $\{f_{e_1}, f_{e_2}, ..., f_{e_{k'}}\}$ forms a set of linear independent vectors and assume that it is the set of eavesdropped channels. Then the information transmitted on the k' channels will be $\mathbf{x}'Q^{-1}Gf_{e_1}, \mathbf{x}'Q^{-1}Gf_{e_2}, ..., \mathbf{x}'Q^{-1}Gf_{e_{k'}}$ respectively. Or equivalently

$$\mathbf{x}'Q^{-1}f'_{e_1}, x'Q^{-1}f'_{e_2}, ..., x'Q^{-1}f'_{e_k} \tag{4.16}$$

where $f'_{e_l} = Gf_{e_l}, \forall 1 \leq l \leq k'$. Next, we are going to show by contradiction that all the symbols the eavesdropper obtains from the channels are a mixture of the symbols from X and R, and that the eavesdropper cannot recover any information about X, either completely or partially. To extract any kind of information consisting only symbols from X, there must exist at least one vector f in the vector space $\left\langle f'_{e_1}, f'_{e_2}, ..., f'_{e_{k'}} \right\rangle$ such that

$$Q^{-1}f \in V' \tag{4.17}$$

where V' is the vector space consisting of all $(\omega+k)$-dimensional column vectors which contain only zeros starting from the $(\omega + 1)$st position. If such a vector f does exist, then

$$f \in V'' \tag{4.18}$$

where $V'' = \{Qv : v \in V'\}$.

And

$$\begin{align} V'' &= \{Qv : v \in V'\} \tag{4.19} \\ &= \langle \{Q\delta_1, Q\delta_2, \ldots, Q\delta_\omega\} \rangle \tag{4.20} \\ &= \langle \{b_1, b_2, ..., b_\omega\} \rangle , \tag{4.21} \end{align}$$

where $\delta_i, 1 \leq i \leq \omega$ is the $(\omega + k)$-dimensional column vector which contains only zeros except in the ith position which is equal to 1.

Therefore,

$$f \in \langle \{b_1, b_2, ..., b_\omega\} \rangle . \tag{4.22}$$

This contradicts (4.4). Therefore, such vector f does not exist. And all the symbols that the eavesdropper obtains from the channels are a mixture of the symbols from X and R.

Let Y_W be the vector of symbols transmitted on the k' eavesdropped channels. Let $\mathbf{y}_W$ be the value of Y_W when $X = (\mathbf{x}, \mathbf{r})$. The information transmitted on the k' eavesdropped channels are

$$\begin{aligned} Y_W =& (\mathbf{x}, \mathbf{r}) \begin{bmatrix} Q^{-1}f'_{e_1} & Q^{-1}f'_{e_2} & \cdots & Q^{-1}f'_{e_{k'}} \end{bmatrix} && (4.23) \\ =& (\mathbf{x}, \mathbf{r}) \begin{bmatrix} G_1 \\ G_2 \end{bmatrix} && (4.24) \\ =& \mathbf{x}G_1 + \mathbf{r}G_2 && (4.25) \end{aligned}$$

where G_1 and G_2 are matrices with dimensions $\omega \times k'$ and $k \times k'$ respectively. Next, we are going to show that the rank of G_2 must be k', equals the number of columns of G_2. Assume that the rank of G_2 is less than k'. There must exist a k'-dimensional non-zero column vector v such that,

$$G_2 v = 0. \tag{4.26}$$

And

$$Y_W v = (\mathbf{x}, \mathbf{r}) \begin{bmatrix} G_1 \\ G_2 \end{bmatrix} v \tag{4.27}$$

$$= (\mathbf{x}, \mathbf{r}) \begin{bmatrix} G_1 v \\ 0 \end{bmatrix} \tag{4.28}$$

$$= \mathbf{x} G_1 v. \tag{4.29}$$

This contradicts the fact that all symbols obtained by the eavesdropper are mixture of the symbols from X and R. Therefore, the rank of G_2 must be k'.

For all subset W of k' channels, $\mathbf{y}_W \in \mathbb{F}^{k'}$ and $\mathbf{x} \in \mathbb{F}^{\omega}$,

$$Pr\{Y_W = \mathbf{y} | X = \mathbf{x}\} \tag{4.30}$$

$$= Pr\{\mathbf{x} G_1 + R G_2 = \mathbf{y}\} \tag{4.31}$$

$$= Pr\{R G_2 = \mathbf{y} - \mathbf{x} G_1\} \tag{4.32}$$

$$= |\mathbb{F}|^{-k'} \tag{4.33}$$

which is independent of $\mathbf{x}$.

Therefore,

$$I(X; Y_W) = 0. \tag{4.34}$$

From now on, we assume that error can happen on all the edges in the network and we will prove that under this situation, the eavesdropper can still not obtain any useful information. Let $\mathcal{E} = \{1, 2, \ldots, |\mathcal{E}|\}$, where the indexing is consistence with the partial order of edges in the

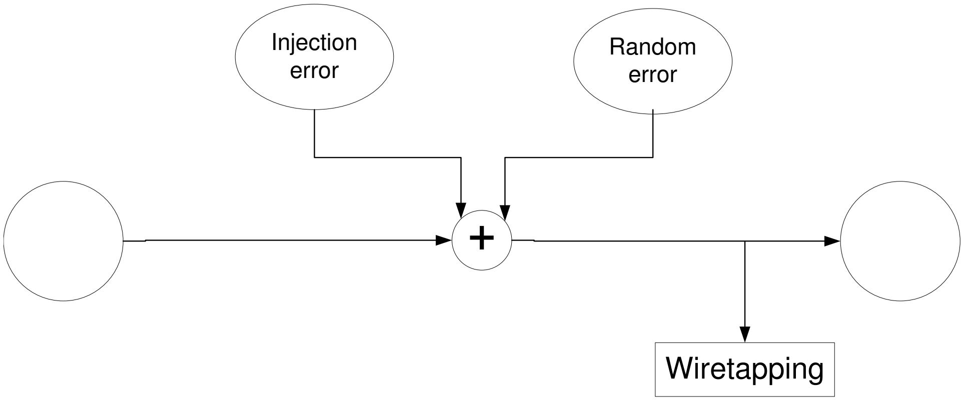


Figure 4.1: error components and wiretapping of the edge j

network.

Assume that on each edge $i \in \mathcal{E}$, the error is an addition of two components, as illustrated in Figure 4.1. One of the component is called random error Z_i^{ran} which is not under the control of the adversary and satisfies

$$I(X, R; Z^{ran}) = 0., \tag{4.35}$$

where $Z^{ran} = (Z_i^{ran}, 1 \leq i \leq |\mathcal{E}|)$. And we assume that the adversary is powerful enough to know all the random errors Z^{ran} injected though the value of the random errors are out of adversary's control.

Let $\{\sigma(1), \sigma(2), \ldots, \sigma(k)\}$ be the set of k channels that the adversary chooses to eavesdrop where the indexing is consistence with the partial order of the edges in the network. In order words, $\sigma(i) \leq \sigma(j), \forall i < j$. Assume that $\forall 1 \leq j \leq |\mathcal{E}|$, there exists $1 \leq i_j \leq k$ such that either $\sigma(i_j) < j$ and $j \leq \sigma(i_j + 1)$, or $\sigma(i) < j, \forall 1 \leq i \leq |\mathcal{E}|$. And we assume that the adversary has the ability to decide what errors to be injected into the downstream of the network based on the information it obtained in the upstream.

Let $Y_j, 1 \leq j \leq k$, be the symbols transmitted on the edge $\sigma(j)$ when there is no error injected into the network and let $Y'_j, 1 \leq j \leq k$, be the symbols transmitted on the edge $\sigma(j)$ when there are errors in the network (either random or injected). We further assume that for every channel chosen, the eavesdropper always eavesdrops at the receiving end of the channel, that is, after the errors are injected if there is any. This assumption can be justified because in our model, the adversary are assumed to know not only the injected errors, but also the random errors that are happening on every channels. The information that the adversary can obtain by eavesdropping the receiving end of the channels allows it to calculate the information at the transmitting end of the channels. Therefore $\forall j, 1 \leq j \leq k$,

$$Y'_j = Y_j + g'_j(Z_i^{in}, Z_i^{ran}, \forall i \leq \sigma(j),) \tag{4.36}$$

where $g'_e(\cdot)$s are deterministic functions depend only on the local encoding kernels of the network.

Then $\forall j, 1 \leq j \leq k$,

$$\begin{aligned}
&I(Z_j^{in}; Y_{i_j+1}, \ldots, Y_k | Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) \\
=&I(Z_j^{in}; Y_{i_j+1}, \ldots, Y_k | Y'_1, \ldots, Y'_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) && (4.37) \\
\leq&I(Z_j^{in}; X, R | Y'_1, \ldots, Y'_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) && (4.38) \\
=&0. && (4.39)
\end{aligned}$$

where the first equality is valid because when $(Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran})$ are all known, the values of $Y_1, \ldots, Y_{i_j}$ can always be calculated from $Y'_1, \ldots, Y'_{i_j}$ by using equation (4.36) and vice versa, the first inequality comes from the fact that $Y_{i_j+1}, \ldots, Y_k$ are all functions of X, R and the last equality is true by the construction of our model. Therefore, $\forall j, 1 \leq j \leq k$,

$$I(Z_j^{in}; Y_{i_j+1}, \ldots, Y_k | Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) = 0. \tag{4.40}$$

Also $\forall j, 1 \leq j \leq k$,

$$\begin{aligned} & I(Z_j^{in}; Y_{i_j+1}, \ldots, Y_k | X, R, Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) \\ \leq & I(Z_j^{in}; X, R | X, R, Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) \qquad (4.41) \\ = & 0. \qquad (4.42) \end{aligned}$$

Therefore, $\forall j, 1 \leq j \leq k$,

$$I(Z_j^{in}; Y_{i_j+1}, \ldots, Y_k | X, R, Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) = 0. \tag{4.43}$$

Then $\forall j, 1 \leq j \leq k$,

$$\begin{aligned} & I(X, R; Z_j^{in} | Y_1, \ldots, Y_{i_j}, Y_{i_j+1}, \ldots, Y_k, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) \\ = & I(X, R; Z_j^{in} | Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) - \\ & I(X, R; Z_j^{in}; Y_{i_j+1}, \ldots, Y_k | Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) \qquad (4.44) \\ = & I(X, R; Z_j^{in} | Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) - \\ & I(X, R; Z_j^{in}; Y_{i_j+1}, \ldots, Y_k | Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) - \\ & I(Z_j^{in}; Y_{i_j+1}, \ldots, Y_k | X, R, Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) \qquad (4.45) \\ = & I(X, R; Z_j^{in} | Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) - \\ & I(Z_j^{in}; Y_{i_j+1}, \ldots, Y_k | Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) \qquad (4.46) \\ = & I(X, R; Z_j^{in} | Y_1, \ldots, Y_{i_j}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) \qquad (4.47) \\ = & 0 \qquad (4.48) \end{aligned}$$

where equation (4.45) comes from equation (4.43), equation (4.47) comes from equation (4.40) and the last equality is valid by the construction of our model. (4.44) comes from the following equation

$$I(A;B;C) = I(A;C) - I(A;B|C)^{1}. \tag{4.49}$$

Since $Y_{\mathrm{W}} = (Y_1, \ldots, Y_k)$, it follows from (4.48) that

$$I(X, R; Z_j^{in}|Y_{\mathrm{W}}, Z_1^{in}, \ldots, Z_{j-1}^{in}, Z^{ran}) = 0 \tag{4.50}$$

By summing over all j, and applying the chain rule for mutual informatoin, we get

$$\begin{aligned} & I(X, R; Z^{in}|Y_{\mathrm{W}}, Z^{ran}) \\ =& \sum_j I(X, R; Z_j^{in}|Y_{\mathrm{W}}, Z_1, \ldots, Z_{j-1}, Z^{ran}) && (4.51) \\ =& 0. && (4.52) \end{aligned}$$

where $Z^{in} = (Z_i^{in}, 1 \leq i \leq |\mathcal{E}|)$.

[1] See [31]

On the other hand,

$$\begin{aligned}
& I(X;Y_{\mathrm{W}}|Z^{ran}) \\
=& I(X;Y_{\mathrm{W}}) - I(X;Y_{\mathrm{W}};Z^{ran}) && (4.53) \\
=& - I(X;Y_{\mathrm{W}};Z^{ran}) && (4.54) \\
=& I(X;Z^{ran}|Y_{\mathrm{W}}) - I(X;Z^{ran}) && (4.55) \\
=& I(X;Z^{ran}|Y_{\mathrm{W}}) && (4.56) \\
\leq& I(X,R;Z^{ran}|Y_{\mathrm{W}}) && (4.57) \\
=& I(X,R;Z^{ran}) - I(XR;Z^{ran};Y_{\mathrm{W}}) && (4.58) \\
=& - I(X,R;Z^{ran};Y_{\mathrm{W}}) && (4.59) \\
\leq& I(Z^{ran};Y_{\mathrm{W}}|X,R) && (4.60) \\
\leq& H(Y_{\mathrm{W}}|X;R) && (4.61) \\
=& 0 && (4.62)
\end{aligned}$$

where equation (4.54) comes from equation (4.34), both equations (4.56) and (4.59) come from equation (4.35) and equation(4.60) follows from

$$\begin{aligned}
0 \leq& I(Z^{ran};Y_{\mathrm{W}}) && (4.63) \\
=& I(X,R;Z^{ran};Y_{\mathrm{W}}) + I(Z^{ran};Y_{\mathrm{W}}|X,R). && (4.64)
\end{aligned}$$

Since $I(X;Y_{\mathrm{W}}|Z^{ran}) \geq 0$, (4.62) implies

$$I(X;Y_{\mathrm{W}}|Z^{ran}) = 0. \tag{4.65}$$

Therefore,

$$
\begin{aligned}
&I(X; Y_{\mathrm{W}}, Z^{in}, Z^{ran}) \\
=&I(X; Z^{ran}) + I(X; Y_{\mathrm{W}}|Z^{ran}) + I(X; Z^{in}|Y_{\mathrm{W}}, Z^{ran}) && (4.66) \\
=&I(X; Y_{\mathrm{W}}|Z^{ran}) + I(X; Z^{in}|Y_{\mathrm{W}}, Z^{ran}) && (4.67) \\
=&I(X; Z^{in}|Y_{\mathrm{W}}, Z^{ran}) && (4.68) \\
=&0. && (4.69)
\end{aligned}
$$

where equation (4.67) comes from equation (4.35), equation (4.68) comes from equation (4.65), and equation (4.69) comes from equation (4.52).

Finally,

$$
\begin{aligned}
&I(X; Y'_{\mathrm{W}}) \\
\leq&I(X; Y'_{\mathrm{W}}, Z^{in}, Z^{ran}) && (4.70) \\
=&I(X; Y_{\mathrm{W}}, Z^{in}, Z^{ran}) && (4.71) \\
=&0. && (4.72)
\end{aligned}
$$

Therefore,

$$
I(X; Y'_{\mathrm{W}}) = 0, \tag{4.73}
$$

This is, the code we constructed in the last section is indeed secure. □

Next, we are going to prove that $m-2d-k$ is an upper bound on the multicast rate of secure error-correcting network code in the presence of an adversary that can inject d errors and eavesdrop k channels. In establishing this result, we need a set of inequalities due to Han [47] stated in the next lemma.

Lemma 4.1. *([13]) For a subset α of $\mathcal{N} = \{1, 2, \ldots, m\}$, let $\bar{\alpha} = \mathcal{N} \backslash \alpha$ and $(X_i, i \in \alpha)$ by X_α. For $1 \leq k \leq m$, let*

$$H'_k = \frac{1}{\binom{m-1}{k-1}} \sum_{\alpha:|\alpha|=k} H(X_\alpha | X_{\bar{\alpha}}). \tag{4.74}$$

Then

$$H'_1 \leq H'_2 \leq \cdots \leq H'_m. \tag{4.75}$$

Theorem 4.2. *The maximum rate at which information can be transmitted from the source node to all sink nodes with linear network code in the presence of adversary that can eavesdrop k channels and inject d errors at the same time is $m - 2d - k$.*

Proof. Let t be the sink node such that there exists a cut U between s and t such that the there are exactly m edges across the cut U. Let $\mathcal{E}_t = \{e_1, e_2, \ldots, e_m\}$ be the set of edges across the cut U. Assume that the source node transmits ω units of information, $\mathbf{x} = \{x_1, x_2, \ldots, x_\omega\}$, to the sink nodes and k' symbols of randomness are introduced.

Consider a fixed linear network code in which all the node will transmit a linear combination of the information that it received from the incoming edges onto the outgoing edges according to the local encoding kernels. Then the information transmitting across the cut is,

$$\mathbf{x}G_M + \mathbf{r}G_R \tag{4.76}$$

where G_M is a $\omega \times m$ generator matrix for the message and G_R is a $k' \times m$ matrix and the exact value of G_M and G_R depend on the local encoding kernels of the linear network code considered. The rank of G_M must be ω for the message to be decodable at the sink nodes. Also,

$$\langle G_M \rangle \cap \langle G_R \rangle = \{0\} \tag{4.77}$$

where $\langle G_M \rangle$ and $\langle G_R \rangle$ are the row vector spaces of G_M and G_R respectively. Otherwise, there exists a $\mathbf{x}, \mathbf{x}' \in \mathbb{F}^{\omega}, \mathbf{x} \neq \mathbf{x}', \mathbf{r}, \mathbf{r}' \in \mathbb{F}^{k}, \mathbf{r} \neq \mathbf{r}'$, such that

$$(\mathbf{x} - \mathbf{x}')G_M = (\mathbf{r} - \mathbf{r}')G_R. \tag{4.78}$$

This implies

$$\mathbf{x}G_M + \mathbf{r}'G_R = \mathbf{x}'G_M + \mathbf{r}G_R. \tag{4.79}$$

Then, the sink node t would not be able to decode the message correctly.

Assume information is transmitting at the rate of $L - a$ and a units of randomness, $\mathbf{r} = \{r_1, r_2, \dots r_a\}$, are introduced where $L > a$. Next we are going to show that at least k symbols of randomness are required for the code to be secured.

We first deal with the case when $L \geq k + 1$. Let $Y_{\mathcal{E}'}, \mathcal{E}' \subset \mathcal{E}$, be the vector of symbols transmitted on the edge in $\mathcal{E}'$. We first assume that G_R is a full rank matrix, since $\langle G_M \rangle \cap \langle G_R \rangle = \{0\}$,

$$\begin{bmatrix} G_M \\ G_R \end{bmatrix} \text{ is a full rank matrix.} \tag{4.80}$$

Therefore, $\exists$ an $L \times L$ submatrix which is invertible. This implies there exists a subset $\mathcal{E}_t' \subset \mathcal{E}_t, |\mathcal{E}_t'| = L$, such that

$$H(X, R|Y_{\mathcal{E}_t'}) = 0. \tag{4.81}$$

This further implies

$$H(X|Y_{\mathcal{E}_t'}) = 0. \tag{4.82}$$

For the case in which $rank(G_R) = b < a$, there exists a matrix $\hat{G}_R$ that consists of b rows of G_R such that $\forall \mathbf{x} \in \mathbb{F}^{L-a}, \mathbf{r} \in \mathbb{F}^a$, $\exists \mathbf{r}' \in \mathbb{F}^b$ such that

$$(\mathbf{x}, \mathbf{r}) \begin{bmatrix} G_M \\ G_R \end{bmatrix} = (\mathbf{x}, \mathbf{r}') \begin{bmatrix} G_M \\ \hat{G}_R \end{bmatrix} \tag{4.83}$$

where components of $\mathbf{r}'$ is a linear combination of components of $\mathbf{r}$. Since $\langle G_M \rangle \cap \langle G_R \rangle = \{0\}$, $\exists$ an $(L - a + b) \times (L - a + b)$ submatrix which is invertible. This implies there exists a subset $\mathcal{E}_t' \subset \mathcal{E}_t, |\mathcal{E}_t'| = L$, such that

$$H(X, R'|Y_{\mathcal{E}_t'}) = 0 \tag{4.84}$$

where $\mathbf{r}'$ is the outcome of the random variable R'. This further implies

$$H(X|Y_{\mathcal{E}_t'}) = 0. \tag{4.85}$$

For any $\mathcal{I} \subset \mathcal{E}'_t, |\mathcal{I}| = k$, consider

$$\begin{aligned} H(X) &= H(X|Y_{\mathcal{E}'_t}) + I(Y_{\mathcal{E}'_t}; X) && (4.86) \\ &= I(Y_{\mathcal{I}}; X) + I(Y_{\mathcal{E}'_t \backslash \mathcal{I}}; X|Y_{\mathcal{I}}) && (4.87) \\ &= I(Y_{\mathcal{E}'_t \backslash \mathcal{I}}; X|Y_{\mathcal{I}}) && (4.88) \end{aligned}$$

where the second equality comes from equation (4.82) and the last equality comes from the requirement for the code to be secured. Summing over all $\mathcal{I}$, we have

$$\begin{aligned} & \begin{pmatrix} L \\ k \end{pmatrix} H(X) \\ &= \sum_{\mathcal{I}} I(Y_{\mathcal{E}'_t \backslash \mathcal{I}}; X|Y_{\mathcal{I}}) && (4.89) \\ &\leq \begin{pmatrix} L-1 \\ L-k-1 \end{pmatrix} \left[\frac{1}{\binom{L-1}{L-k-1}} \sum_{\mathcal{I}} H(Y_{\mathcal{E}'_t \backslash \mathcal{I}}|Y_{\mathcal{I}}) \right] && (4.90) \\ &\leq \begin{pmatrix} L-1 \\ L-k-1 \end{pmatrix} H(Y_{\mathcal{E}'_t}), && (4.91) \end{aligned}$$

where the last inequality follows from Lemman 4.1. Hence,

$$H(Y_{\mathcal{E}'_t}) \geq \frac{L}{L-k} H(X). \qquad (4.92)$$

Finally,

$$\begin{aligned} H(X) + H(R) &\geq H(X, R) && (4.93)\\ &= H(X, R, Y_{\mathcal{E}'_t}) && (4.94)\\ &\geq H(Y_{\mathcal{E}'_t}) && (4.95)\\ &\geq \frac{L}{L-k} H(X) && (4.96) \end{aligned}$$

where equality (4.94) comes from

$$H(Y_{\mathcal{E}'_t} | X, R) = 0. \tag{4.97}$$

This implies

$$H(R) \geq \frac{k}{L-k} H(X) \geq k \tag{4.98}$$

where X is uniformly distributed. Therefore, at least k symbols of randomness are needed to be introduced.

On the other hand, when $L \leq k$, there exists a subset $\mathcal{E}'_t \subset \mathcal{E}_t$, $|\mathcal{E}'_t| = k$, such that

$$H(X, R | Y_{\mathcal{E}'_t}) = 0. \tag{4.99}$$

The code is insecure. Therefore, at least k symbols of randomness are needed to be introduced.

Now, assume that k symbols of randomness are introduced. For the network code to correct any d errors injected into $\mathcal{E}_t$, $\forall \mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}^\omega, \mathbf{x}_1 \neq$

$\mathbf{x}_2, \mathbf{r}_1, \mathbf{r}_2 \in \mathbb{F}^k$, and $z_1, z_2 \in \mathbb{F}^m, |z_1| \leq d, |z_2| \leq d$,

$$\begin{aligned} &\mathbf{x}_1 G_M + \mathbf{r}_1 G_R + z_1 \\ &\neq \mathbf{x}_2 G_M + \mathbf{r}_2 G_R + z_2. \end{aligned} \tag{4.100}$$

Or $\forall \mathbf{x} \in \mathbb{F}^\omega, \mathbf{x} \neq 0$,

$$\mathbf{x} G_M \notin \{\mathbf{r} G_R + z : \mathbf{r} \in \mathbb{F}^k, z \in \mathbb{F}^m, |z| \leq 2d\} \tag{4.101}$$

Let

$$G'_R = \begin{bmatrix} g_{r,1} \\ g_{r,2} \\ \vdots \\ g_{r,k} \end{bmatrix} \tag{4.102}$$

be the row-echelon form of G_R. We can always find $2d$ vectors, namely $v_1, v_2, \ldots, v_{2d}$, from the set of standard basis of $\mathbb{F}^m$ such that

$$\{g_{r,1}, g_{r,2}, \ldots, g_{r,k}, v_1, v_2, \ldots, v_{2d}\} \tag{4.103}$$

forms a set of $k + 2d$ linear independent vectors. Therefore,

$$\left|\{\mathbf{r} G_R + z : \mathbf{r} \in \mathbb{F}^k, z \in \mathbb{F}^m, |z| \leq 2d\}\right| \tag{4.104}$$

$$\geq |\langle\{g_{r,1}, g_{r,2}, \ldots, g_{r,k}, v_1, v_2, \ldots, v_{2d}\}\rangle| \tag{4.105}$$

$$= |\mathbb{F}|^{k+2d} \tag{4.106}$$

where equation (4.105) comes from the fact that
$\forall \mathbf{y} \in \langle\{g_{r,i}, 1 \leq i \leq k, v_j, 1 \leq j \leq 2d\}\rangle, \exists \mathbf{r} \in \mathbb{F}^k, z \in \mathbb{F}^m, |z| \leq 2d$ such

that $\mathbf{y} = \mathbf{r}G_R + z$.

By equation (4.101), rank of G_M must be less than $m - 2d - k + 1$. Otherwise the sink node cannot decode the information successfully. Therefore, the maximum rate at which information can be transmitted from the source node to all sink nodes must be at most $m - 2d - k$.

□

Next, we will see a simple example illustrating the SEC code. A simple network consisting of one source node s and one sink node t is considered. The source node and sink node are connected by 4 directed edges from s to d. The capacity of this network, therefore, is 4. We will show how the procedure described in the above theorem allows us to construct a SEC code which can transmit a single unit of information without exposing any useful information to the adversary which is assumed to be able to inject a single error into any channel and eavesdrop one of the 4 channels at the same time.

We now construct a 2-dimensional linear network code over $GF(5)$ by assigning the vector $\binom{1}{1}$, $\binom{1}{2}$, $\binom{1}{3}$ and $\binom{1}{4}$ to the 4 channels as global encoding vectors. The received vector for the sink node is

$$\mathbf{y} = \mathbf{x}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} + \mathbf{z}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{4.107}$$

With such an assignment, one can verify easily that the resulting network code is an error-correcting network code with distance 3. Since we have to ensure that the adversary would not obtain any useful information by eavesdropping any 1 of the 4 channels and the source node need to transmit a unit of information to the sink node, we now have to choose, according to Theorem 4.1, a 2-dimensional vector which is linearly independent to any 1 of the 4 global encoding vector of the 4 channels. $\binom{1}{0}$ is such a vector. We then construct the invertible matrix

$$Q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{4.108}$$

from the chosen $\binom{1}{0}$.

According to Theorem 4.1, the transfer matrix will now become

$$\begin{aligned} & Q^{-1} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix} & (4.109) \\ = & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}. & (4.110) \end{aligned}$$

Therefore, the information transmitting in the 4 channels will now be $x+r$, $x+2r$, $x+3r$ and $x+4r$ respectively, where x is the information unit to be transmitted and r is a number taken randomly in $GF(5)$. Since information in all channels are mixed with random data, the adversary will not be able to get any useful information by eavesdropping any 1 of the 4 channels.

4.2 Secret Channel Based Transmission Schemes

In a secret channel, a transmission can be completely free from eavesdropping by the adversary while at the same time the data can still reach all the sink nodes despite any corrupted data the adversary injects into the network. Such channel can be realized by applying the SEC network code proposed in Section 4.1. Such a secret channel works under the condition $2d + k < m$. The maximum rate at which source node can multicast information to the sink nodes is $m-2d-k$. In [25], a scheme based on random network coding [26] has been proposed which can also achieve the capacity of $m-d$ with a looser constraint $d+k < m$, but with a bigger sacrifice on bandwidth in the initial stage of secret data transmission.

By using the secret channel created, we discuss the following three transmission schemes. The first two schemes can achieve the rate $m-d$. In the presence of feedback, the third scheme can possibly achieve a rate higher than $m - d$ based on the usage of a feedback channel. To simplify our discussion, we assume that $m_t = m$ for all sink node t in this section. But our results apply to the general cases.

In the first scheme, we will use the secret channel to transmit a parity check matrix and the hashed data created from the source information to be transmitted. These information will later be proved to be useful in decoding the source information at the sink nodes. In the second scheme, we use the secret channel to notify the sink nodes the time slots during which information will be transmitted at a lower data rate. In this scheme, we have to assumed that the adversary will inject errors into the network randomly. In the third scheme, we assume that there exists feedback channels between the sink nodes and the source node.

4.2.1 Hash Code

This scheme is originally proposed and shown to be feasible with a very high successful rate in [23] with the usage of random network code. By using deterministic code, this scheme can be modified and greatly simplified. Also, due to the deterministic nature of the code that we will construct, it turns out that the sink nodes will be able to decode the data they received with a higher probability of success.

The scheme goes as follows. The source node will first generate a secret message which will then be transmitted through the secret channel. Firstly, we have to accumulate $h(m-d)$ source information where h is large comparing to m. Then we construct a $h \times (m-d)$ matrix S using the source information accumulated. Secondly, the source node will then chooses m parity symbols uniformly from the field $\mathbb{F}$. The parity symbols are labeled r_d, for $d \in \{1, 2, ..., m\}$. Then a m by h matrix P is defined whose $(i, j)th$ entry equals to $(r_i)^j$. The second part of source node's secret message is a m by $m-d$ hash matrix H, computed as the matrix product PS. The source node will then transmit both the set of parity symbols and the hash matrix H to all sink nodes over the security channel. After that, the source message will then be multicast to the sink nodes with a $m-d$ dimensional network code with distance $d+1$. Such a code can be constructed without modifying the local encoding kernels of the nodes by applying the algorithm proposed in Theorem 5 in [27].

A corresponding matrix Y_t will then be constructed by every sink node, with the message it received. That is,

$$Y_t = SGF_{s,t} + ZF_t \tag{4.111}$$

where G is the generator matrix for the message set and Z is the h by $|\mathcal{E}|$ matrix composed of the error vectors of each time slots as its row vectors.

Every sink node t will then computed

$$PY_t - PSGF_{s,t} = PZF_t. \tag{4.112}$$

It can be proved [17] that, with very high probability, the rows of PZF_t span the same vector space as the rows of ZF_t. Therefore, ZF_t can be written as a linear combinations of the rows of PZF_t. Let D be the matrix whose row vector form an arbitrary set of basis vector generating the row space of PZF_t. This allows the sink node to rewrite (4.111) as the matrix product

$$Y_t = \begin{bmatrix} S & A \end{bmatrix} \begin{bmatrix} GF_{s,t} \\ D \end{bmatrix}. \tag{4.113}$$

where A is a certain matrix when appropriate dimensions.

If the matrix $\begin{bmatrix} GF_{s,t} \\ D \end{bmatrix}$ has full row rank, there will be a one-to-one mapping between Y_t and $\begin{bmatrix} S & A \end{bmatrix}$. The corresponding sink node can then recover the message matrix S correctly.

Lemma 4.2. *Given any network code with minimum distance* $d + 1$

with transfer matrix F, the matrix $\begin{bmatrix} GF_{s,t} \\ D \end{bmatrix}$ *has full row-rank with certainty.*

Proof. Since the row vectors of PZF_t span the same space as the row vectors of ZF_t and D is a set of basis vector generating the row space of PZF_t, it is sufficient to show that $\langle GF_{s,t}\rangle$ and $\langle ZF_t\rangle$ are disjoint vector spaces, where $\langle GF_{s,t}\rangle$ and $\langle ZF_t\rangle$ represent the row vector spaces of the matrices $GF_{s,t}$ and ZF_t respectively. We will show this by contradiction. Suppose $\langle GF_{s,t}\rangle \bigcap \langle ZF_t\rangle \neq \emptyset$, and let $\mathbf{v} \in \langle GF_{s,t}\rangle \bigcap \langle ZF_t\rangle$. Therefore, there exists a certain vector $\mathbf{z}$ such that $\mathbf{v} = \mathbf{z}ZF_t$. One the other hand, $\langle GF_t\rangle$ is vector space, for every message vector $\mathbf{x}$ generated by G, there exists a message vector $\mathbf{x}'$ such that

$$\mathbf{x}F_{s,t} + \mathbf{z}ZF_t = \mathbf{x}F_{s,t} + \mathbf{v} = \mathbf{x}'F_{s,t}. \tag{4.114}$$

Therefore, based on the inaction assumption, there exists $\mathbf{z}', w_H(\mathbf{z}') \leq d$,

$$\mathbf{x}F_{s,t} + \mathbf{z}'F_t = \mathbf{x}'F_{s,t}. \tag{4.115}$$

This contradicts the fact that the given network coding is a network code with minimum distance $d+1$. □

In order to obtain the optimal rate of $m-d$, h needs to be large comparing to m so as to make the secret message negligible. However, in making h arbitrarily large, the probability that matrix D successfully spanning the row vector space of ZF_t can be diminished. In order to balance out this negative effect, the field size q need also to be arbitrarily large. In this scheme, the source node needs to store at least

$(m - d) \times h$ source symbols, with each of them in $\mathbb{F}$, for each single batch of data. The memory requirement for the source node can then be substantially large.

By making extra assumption, we are going to propose another simple scheme that can asymptotically achieve the optimal capacity of $m - d$ in which the memory requirement for the source node is smaller.

4.2.2 Training Transmission Scheme

As discussed in [22], if the sink nodes have the knowledge of the active error pattern, the error becomes an erasure and the code can have twice the error correction ability. On the other hand, for the errors with the same weight d, if the error pattern can be obtained by the sink nodes, source node can increase its transmission rate from $m - 2d$ to $m - d$. The main issue is how to obtain the erasure pattern at the sink nodes.

For a fixed erasure pattern ρ, the observed error $\mathbf{z}F_t$ at sink node t must lie in a subspace of $\mathbb{F}^{n_t}$, say $Z_{\rho,t}$ where n_t is the number of incoming edges of the node t. It is possible to estimate $Z_{\rho,t}$ if an enough number of $\mathbf{z}F_t$ was received at the sink nodes. However, if the adversary changes the set of channels to inject errors in every transmission of the network, in the worst case, no information about the error pattern can be estimated. Thus, we assume the adversary is inactive, i.e., the adversary uses the same set of channels for a long enough period of time. Assume $|\rho| \leq d$. Before knowing ρ, source node s transmits at rate $m - 2d$ and each sink node can decode correctly. Thus $\mathbf{z}F_t = \mathbf{y}_t - \mathbf{x}F_{s,t}$ can be calculated at each sink node t. If ρ remains unchanged for a period of time, the $Z_{\rho,t}$ can then be estimated and reconstructed with a very high accuracy.

Thus we can have a transmission scheme based on the error pattern estimation. The source node first transmit a mount of information at rate $m-2d$. Sink nodes can decode such information correctly and use the received vectors to estimate the error pattern. These transmissions are called training. After the error pattern is estimated. Then the source node transmit at rate $m-d$, and sink nodes can decode the information correctly by erasure correction. In our scheme we do not need to change the local encoding kernels but only the message set. For a fix set of local encoding kernels, different rate of message set can be constructed by the algorithm in [27].

However, there is a security problem in our transmission scheme. We should prevent the adversary from knowing the training pattern, the set of time slots during which the data is transmitted at the lower rate of $m-2d$. If the adversary does know the training pattern, it can disguise itself. For example, the adversary may inject the same corrupted packets into the network for training transmission. In this way, all the sink nodes would only be able to recover at most a 1-dimensional subspace of $Z_{\rho,t}$. Thus we need a secret channel which cannot be eavesdropped by the adversary to transmit the training pattern from the source node to all the sink nodes.

At the very beginning of the communication, the source nodes will notify, using the security channel, all sink nodes the next time slot during which the source node will transmit information with lower rate, $m-2d$, so that the sink nodes can be prepared and then recover both the data and the error vectors without acknowledged by the adversary. Also, by embedding the information about the next training time slot into the data being multicast in this time slot, the source node can at the same time notify the sink nodes when the next training time slot will be.

Since the adversary cannot determine when the training time slot will be, we further assume that the adversary will randomly choose some corrupted data to be injected into the network. This scheme makes sure that when the field size and the number of training time slot is large enough, all sink nodes will be able to, with very high probability, receive and recover data from the source node at the rate $m - d$.

4.2.3 Secret Channel Model With Feedback

In the presence of feedback, the rate at which information can be multicast from the source node to the sink nodes can be increased beyond $m-d$ as obtained before. The main contribution here is to achieve the better result here without reconstructing the network code. In fact, the result can be achieved by just changing the message set at the source node while the local encoding kernels of all nodes in the network remain unchanged. In the previous section, we have shown that after a long enough time, we can reconstruct with a high probability the whole vector space of errors that can be imposed onto each sink node by the malicious party. By notifying the source node about the error vector spaces received by each sink node using the feedback channels, depending on the maximum dimension of error that is received by every sink node, the source node may be able to increase the multicast rate further. Here we assume that the feedback channels are error-free. Since the sink nodes only need to feedback the information of error space once over the very long period of time, the capacity of these feedback channels can be assumed to be negligible compared with the forward channels.

By applying an algorithm similar to that in Theorem 5 in [27], we can obtain the following Corollary.

Corollary 4.1. *Given a linear multicast N which can correct network erasures with weight less than or equal to d, there exists, in the presence of feedback channels from sink nodes to source node, a suitable generator matrix for the message set with which source node can multicast data at the rate of*

$$\min_{t \in \mathcal{T}} \left(m_t - u_t \right). \tag{4.116}$$

where u_t is the dimension of the reconstructed error vector space received by sink node t.

4.3 Conclusion

In this chapter, an algorithm in constructing a deterministic secure error-correcting (SEC) network code is proposed. We have shown that in the presence of malicious parties, by combining the idea of secure network code and error-correcting network code, information still can be multicast with complete secrecy and error tolerability at the rate of $m - 2d - k$, where k and d are the maximum number of channels the adversary can eavesdrop and contaminate respectively. We further show that by applying the so constructed network code to create a temporary secure channel, different schemes can then be proposed with which a higher multicast rate of $m-d$ can be obtained with a very high probability. At last, we also show that with the presence of feedback channels from the sink nodes to the source node, data rate can be further boosted beyond $m-d$, without further modification of the existing network code, depending on the maximum dimension of errors the adversary can impose upon every sink nodes.

□ **End of chapter.**

Chapter 5

Network Generalized Hamming Weight

Summary

In this chapter, we extend the notion of generalized Hamming weight for classical linear block code proposed by Wei [9] to linear network codes by proposing a *network generalized Hamming weight (NGHW)* for a given network with respect to a fixed set of global encoding kernel. The basic properties of the NGHW will be studied. We will further show that the NGHW can be used as a tool to characterize the security performance of a linear code on the CSWN. We also introduce the idea of Network Maximum Distance Separation code (NMDS code) by extending the notion of Maximum Distance Separation code in classical algebraic coding theory. We prove that NMDS codes play an important role in minimizing the information that an eavesdropper can obtain from the network. In addition, a one-pass construction of a secure network code will also be given.

Motivated by the work of Wei on generalized Hamming weight for linear block codes [9], which has connections with wiretap channel II [8] and secure sharing model proposed independently by Blakley [14] and Shamir [15], and the work of Cai and Yeung on secure network coding [5], we extend the definition of generalized Hamming weight for linear block codes to linear network codes. To be more specific, we will give a new definition of generalized Hamming weight called the *network generalized Hamming weight (NGHW)* for a given network with respect to a fixed set of global encoding kernels of a given linear network code. Based on the NGHW for linear network codes, we can prove the existence of a network extension of the generalized Singleton bound [9]. The tightness of such a generalized Singleton bound will also be proved. Moreover, through the construction of the linear network code that can achieve the generalized Singleton bound induced by network generalized Hamming weight, we can recover the construction of a secure network code in [5–7].

By extending the original definition of the generalized Hamming weight, our network generalized Hamming weight can completely characterize the performance of linear network codes on a communication system on a wiretap network (CSWN) [5], which includes secret sharing in classical cryptography as a special case.[1] The details of this application are contained in Section 5.3.

[1] The wiretap channel II is a special case of secret sharing.

5.1 Definitions

Wei [9] introduced the notion of the generalized Hamming weight for the classical point-to-point channel which is closely related to the security of data transmission in the wiretap channel II model. He showed that in the case of coset coding, generalized Hamming weight can be used to completely characterize the code performance on the wiretap channel of type II. In this section, by integrating the generalized Hamming weight with network coding, we extend the notion of the generalized Hamming weight to communication networks. In the following, we will first define the network generalized Hamming weight and then prove some of its basic properties.

Definition 5.1. *An n-dimensional linear network code is said to be* full-rank *if there exists a set of n linear independent global encoding kernels.*

Definition 5.2 (Network Generalized Hamming Weight)**.** *Let $\mathcal{C}$ be an $[n, k]$ linear block code. The rth generalized Hamming weight of $\mathcal{C}$, denoted by $d_r(\mathcal{C}, F)$, with respect to a given n-dimensional full-rank linear network code specified by the set of global encoding kernels $F = \{f_e, e \in \mathcal{E}\}$, is defined as*

$$d_r(\mathcal{C}, F) = \min_{W \subset \mathcal{E}} \{|W| : \mathcal{L}_W \textit{ contains some subcode } D \textit{ of } \mathcal{C} \textit{ with dimension } r\}. \tag{5.1}$$

where $\mathcal{L}_W = \langle \{f_e^T, e \in W\} \rangle$. $d_1(\mathcal{C}, F)$ is also denoted by $w_{\min}$.

Note that in (5.1), if $\mathcal{L}_{\mathrm{W}}$ contains some subcode D of $\mathcal{C}$ with dimen-

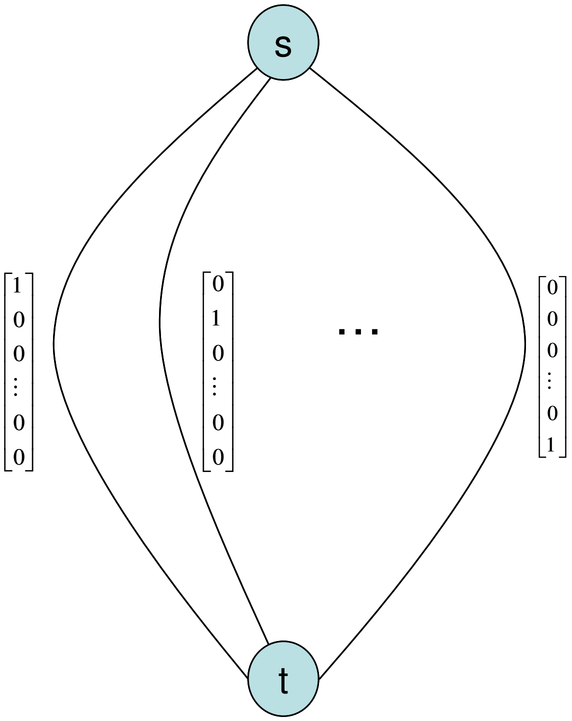


Figure 5.1: A degenerated network consisting of n-channels with $F_{\mathcal{E}} = I$.

sion r, then $dim(\mathcal{C} \cap \mathcal{L}_{\mathrm{W}}) \geq r$.

For $\mathrm{W} \subset \mathcal{E}$, let F_{W} be an $n \times |\mathrm{W}|$ matrix formed by the juxtaposition of $\{f_e, e \in \mathrm{W}\}$. When the network considered is reduced to the network with n channels connecting the source node s and the unique sink node t, and the global encoding kernels forming the $n \times n$ identity matrix, as indicated in Figure 5.1, the definition of $d_r(\mathcal{C}, F)$ reduces to the generalized Hamming weight in [9]. See Section 5.5 for a proof.

In the remainder of this section, we derive several basic properties of the network generalized Hamming weight. Whenever we refer to the NGHW of a linear block code $\mathcal{C}$, we always assume a given full-rank linear network code as prescribed in Definition 5.2.

Lemma 5.1 (Monotonicity)**.** *For an $[n, k]$ linear block code $\mathcal{C}$ with $k >$*

0,

$$1 \leq d_1(\mathcal{C}, F) < d_2(\mathcal{C}, F) < \cdots < d_k(\mathcal{C}, F) \leq n. \tag{5.2}$$

Proof. The inequalities $1 \leq d_1(\mathcal{C}, F)$ and $d_{r-1}(\mathcal{C}, F) \leq d_r(\mathcal{C}, F)$ for $2 \leq r \leq k$ follows directly from Definition 5.2. The inequalities $d_k(\mathcal{C}, F) \leq n$ holds because the given n-dimensional linear network code is full rank. We only need to prove the strict inequalities in (5.2).

For a fixed $2 \leq r \leq k$, let D with $\dim(D) = r$ be a subcode of $\mathcal{C}$ and suppose there exists $\mathrm{W} \subset \mathcal{E}$ such that $d_r(\mathcal{C}, F) = |\mathrm{W}|$ and $D \subset \mathcal{L}_{\mathrm{W}}$.

Let $\langle \mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_r \rangle$ be a basis of D and $\{f_e, e \in \mathrm{W}\} = \{f_{e_1}, f_{e_2}, \ldots, f_{e_{|W|}}\}$. Since $D \subset \mathcal{L}_{\mathrm{W}}$, we may assume that there exists an $r \times |\mathrm{W}|$ matrix $A = \{a_{ij}\}$ such that

$$\begin{bmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_r \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1|\mathrm{W}|} \\ a_{21} & a_{22} & \ldots & a_{2|\mathrm{W}|} \\ \vdots & \vdots & \vdots & \vdots \\ a_{r1} & a_{r2} & \ldots & a_{r|\mathrm{W}|} \end{bmatrix} \begin{bmatrix} f_{e_1}^T \\ f_{e_2}^T \\ \vdots \\ f_{e_{|\mathrm{W}|}}^T \end{bmatrix}. \tag{5.3}$$

Since $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_r \neq 0$, for any $1 \leq i \leq r, 1 \leq j \leq |W|, a_{ij}$ do not all vanish. By reindexing $\{f_{e_1}, f_{e_2}, \ldots, f_{e_{|W|}}\}$ if necessary, we can assume without loss of generality that $a_{r|W|} \neq 0$. We can then obtain

$$\begin{bmatrix} \mathbf{g}'_1 \\ \mathbf{g}'_2 \\ \vdots \\ \mathbf{g}'_{r-1} \\ \mathbf{g}_r \end{bmatrix} = \begin{bmatrix} a'_{11} & a'_{12} & \dots & 0 \\ a'_{21} & a'_{22} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ a'_{(r-1)1} & a'_{(r-1)2} & \dots & 0 \\ a_{r1} & a_{r2} & \dots & a_{r|\mathrm{W}|} \end{bmatrix} \begin{bmatrix} f^T_{e_1} \\ f^T_{e_2} \\ \vdots \\ f^T_{e_{|\mathrm{W}|-1}} \\ f^T_{e_{|\mathrm{W}|}} \end{bmatrix} \tag{5.4}$$

where $\forall 1 \leq i \leq r-1, \mathbf{g}'_i = \mathbf{g}_i - \mathbf{g}_r \frac{a_{1|W|}}{a_{r|W|}}$ and $\forall 1 \leq i \leq r-1, 1 \leq j \leq |W|-1, a'_{ij} = a_{ij} - a_{rj} \frac{a_{1|W|}}{a_{r|W|}}$. It can be readily shown that $\mathbf{g}'_1, \mathbf{g}'_2, \dots, \mathbf{g}'_{r-1}$ are linearly independent. Therefore, there exists an $(r-1)$-dimensional subcode D' of $\mathcal{C}$ with $\mathbf{g}'_1, \mathbf{g}'_2, \dots, \mathbf{g}'_{r-1}$ as the basis such that

$$\begin{bmatrix} \mathbf{g}'_1 \\ \mathbf{g}'_2 \\ \vdots \\ \mathbf{g}'_{r-1} \end{bmatrix} = \begin{bmatrix} a'_{11} & a'_{12} & \dots & a'_{1(|\mathrm{W}|-1)} \\ a'_{21} & a'_{22} & \dots & a'_{2(|\mathrm{W}|-1)} \\ \vdots & \vdots & \vdots & \vdots \\ a'_{(r-1)1} & a'_{(r-1)2} & \dots & a'_{(r-1)(|\mathrm{W}|-1)} \end{bmatrix} \begin{bmatrix} f^T_{e_1} \\ f^T_{e_2} \\ \vdots \\ f^T_{e_{|\mathrm{W}|-1}} \end{bmatrix} \tag{5.5}$$

Therefore,

$$d_{r-1}(\mathcal{C}, F) \leq |\mathrm{W}| - 1 = d_r(\mathcal{C}, F) - 1 < d_r(\mathcal{C}, F) \tag{5.6}$$

□

For an $[n, k]$ linear block code $\mathcal{C}$, denote its $(n-k) \times n$ parity check matrix by $\mathbf{H}$, that is, $\forall \mathbf{c} \in \mathcal{C}, \mathbf{H}\mathbf{c}^T = 0$. The following theorem gives a characterization of $d_r(\mathcal{C}, F)$ in terms of $\mathbf{H}$.

Theorem 5.1.

$$d_r(\mathcal{C}, F) = \min_{W \subset \mathcal{E}} \{|W| : dim(\mathcal{L}_W) - \dim\left(\langle\{\mathbf{H}f_e, e \in W\}\rangle\right) \geq r\} \tag{5.7}$$

Proof. Consider any $\mathrm{W} \subset \mathcal{E}$ that satisfies

$$dim(\mathcal{L}_{\mathrm{W}}) - \dim\left(\langle\{\mathbf{H}f_e, e \in \mathrm{W}\}\rangle\right) \geq r. \tag{5.8}$$

There exists a subset W' of W such that $f_e, e \in \mathrm{W}'$, are linearly independent,

$$dim(\mathcal{L}_{\mathrm{W}'}) = dim(\mathcal{L}_{\mathrm{W}}). \tag{5.9}$$

and

$$\langle\{\mathbf{H}f_e, e \in \mathrm{W}\}\rangle = \langle\{\mathbf{H}f_e, e \in \mathrm{W}'\}\rangle, \tag{5.10}$$

so that (5.8) is satisfied with W' in replace of W. Since $|\mathrm{W}'| \leq |\mathrm{W}|$, in the minimization in (5.7), we only need to consider edge subsets W of which the global encoding kernels are independent of each other, i.e., $dim(\mathcal{L}_{\mathrm{W}}) = |\mathrm{W}|$. A similar arguement shows that the same applies to the minimization in (5.1).

Let $S(\mathrm{W}) = \langle\{\mathbf{H}f_e, e \in \mathrm{W}\}\rangle$ and $S^{ker}(\mathrm{W}) = \left\{\mathbf{c} \in \mathcal{L}_{\mathrm{W}} : \mathbf{H}\mathbf{c}^T = 0\right\}$. We define a linear mapping T from the space of $\langle\{f_e, e \in \mathrm{W}\}\rangle$ to the space of $\langle\{\mathbf{H}f_e, e \in \mathrm{W}\}\rangle$ such that $\forall f_e \in \langle\{f_e, e \in \mathrm{W}\}\rangle, T(f_e) = \mathbf{H}f_e$. Then we have $\dim(S(\mathrm{W})) = \dim(\langle\{f_e, e \in \mathrm{W}\}\rangle) - \dim(ker(T))$ and

$\dim(ker(T)) = \dim(S^{ker}(\mathrm{W}))$. Thus

$$\dim(S(\mathrm{W})) + \dim(S^{ker}(\mathrm{W})) = \dim(\langle\{f_e, e \in \mathrm{W}\}\rangle) = \dim(\mathcal{L}_{\mathrm{W}}). \tag{5.11}$$

Let d be the quantity on the right-hand side of (5.7). Let $\mathrm{W}' \subset \mathcal{E}$ be such that $\dim(\mathcal{L}_{\mathrm{W}'}) = |\mathrm{W}'| = d$, and

$$\dim\left(\mathcal{L}_{\mathrm{W}'}\right) - \dim\left(\langle\{\mathbf{H}f_e, e \in \mathrm{W}'\}\rangle\right) = r' \geq r. \tag{5.12}$$

Then, $\dim(S^{ker}(\mathrm{W}')) = r'$, and $S^{ker}(\mathrm{W}')$ is a subcode of $\mathcal{C}$. Therefore,

$$d_r(\mathcal{C}, F) \leq d_{r'}(\mathcal{C}, F) \leq |\mathrm{W}'| = \dim(\mathcal{L}_{\mathrm{W}'}) = d. \tag{5.13}$$

The last inequality is due to the fact that $S^{ker}(\mathrm{W}')$ is a subcode of $\mathcal{C}$ with dimension r' and $S^{ker}(\mathrm{W}') \subset \mathcal{L}_{\mathrm{W}'}$ (cf. Definition 5.2 with $S^{ker}(\mathrm{W}')$ in place of D). So $d_r(\mathcal{C}, F) \leq d$.

It remains to establish the inequality in the other direction. Let D be a subcode of $\mathcal{C}$ with $\dim(D) = r$ such that $\exists \mathrm{W}' \subset \mathcal{E}, D \subset \mathcal{L}_{\mathrm{W}'}$, and $\dim(\mathcal{L}_{\mathrm{W}'}) = |\mathrm{W}'| = d_r(\mathcal{C}, F)$. Since $D \subset S^{ker}(\mathrm{W}')$,

$$\dim(S^{ker}(\mathrm{W}')) \geq \dim(D). \tag{5.14}$$

Let $\dim(S^{ker}(\mathrm{W}')) = r'$. Then $r' \geq r$. Assume that $r' > r$. Then

$$D \neq S^{ker}(\mathrm{W}'). \tag{5.15}$$

Using the argument for the last inequality in (5.13), we have

$$d_r(\mathcal{C}, F) < d_{r'}(\mathcal{C}, F) \leq |\mathrm{W}'| = \dim(\mathcal{L}_{\mathrm{W}'}) = d_r(\mathcal{C}, F), \tag{5.16}$$

which is a contradiction. Hence, $\dim(S^{ker}(\mathrm{W}')) = r' = r$. By (5.11) with W' in place of W, we obtain

$$dim(\mathcal{L}_{\mathrm{W}'}) - \dim(S(\mathrm{W}')) = r. \tag{5.17}$$

and by comparing equation (5.17) with the inequalities on the right hand side of (5.7), we prove that

$$d \leq |\mathrm{W}'| = d_r(\mathcal{C}, F). \tag{5.18}$$

□

5.2 The Network Generalized Singleton Bound and Network MDS codes

In this section, the idea of network generalized Singleton bound will first be discussed. Later on, we will show the tightness of this bound under two different conditions.

In Section 5.3, we will see that the generalized Hamming weight has a very close relation with the secure performance of a given linear network code. And achieving the generalized Singleton bound is in fact very closely related to achieving the maximum rate of secure linear multicast in the presence of an eavesdropper.

5.2.1 The Network Generalized Singleton Bound

Theorem 5.2 (Generalized Singleton bound). *For an $[n, k]$ linear code $\mathcal{C}$, we have $d_r(\mathcal{C}, F) \leq n - k + r$, for $1 \leq r \leq k$.*

Proof. From (5.2), we can see that $d_k(\mathcal{C}, F) \leq n$. Assume that for r' such that, $1 < r' \leq k, d'_r(\mathcal{C}, F) \leq n - k + r'$ is true. Then by the monotonicity property of the generalized Hamming weight, $d_{r'-1}(\mathcal{C}, F) \leq d'_r(\mathcal{C}, F) - 1 \leq n - k + (r' - 1)$. The theorem is completed. □

In the rest of the chapter, we denote $d_1(\mathcal{C}, F)$ by $w_{\min}$. Note that in the case of classical algebraic coding, $w_{\min}$ is reduced to the minimum Hamming distance of $\mathcal{C}$.

Corollary 5.1. *An $[n, k]$ linear code $\mathcal{C}$ satisfies*

$$|\mathcal{C}| \leq q^{n - w_{\min} + 1}. \tag{5.19}$$

Next, we are going to show that the generalized Singleton bound is tight in the case of linear multicast. The result can then be easily extended to the case of general linear network code. Here the tightness of the generalized Singleton bound has two meanings. The first one is, for a given set of global encoding kernels, we can find a linear code that achieves the tightness of the generalized Singleton bound. The second one is, for a given linear code, we can find a set of global encoding kernels that achieves the generalized Singleton bound.

For two subsets $V_1, V_2 \subset \mathbb{F}_q^n$, their sum is defined by

$$V_1 + V_2 = \{\mathbf{v}_1 + \mathbf{v}_2 : \mathbf{v}_1 \in V_1, \mathbf{v}_2 \in V_2\}. \tag{5.20}$$

Theorem 5.3. *Given any n-dimensional linear multicast over a finite field $\mathbb{F}$, when $|\mathbb{F}| = q$ is sufficiently large, there exists a linear code $\mathcal{C}$*

with $|\mathcal{C}| = q^k$ *such that*

$$w_{\min} = n - k + 1. \tag{5.21}$$

Proof. We start with any given set of global encoding kernels which defines a linear multicast, which is an n-dimensional full-rank linear network code. Let $\mathcal{W}' = \{\mathrm{W} \subset \mathcal{E} : |\mathrm{W}| = n - k\}$.

Now we construct the linear code $\mathcal{C}$. Let $\mathbf{g}_1, \cdots, \mathbf{g}_k \in \mathbb{F}_q^n$ be a sequence of row vectors obtained as follows. For each $i, 1 \leq i \leq k$, choose $\mathbf{g}_i$ such that

$$\mathbf{g}_i \notin \bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}} + \langle \mathbf{g}_1, \cdots, \mathbf{g}_{i-1} \rangle. \tag{5.22}$$

We first prove that $\mathbf{g}_i$ satisfying (5.22) exists if the field size q is sufficiently large. We observe that $\forall i \leq k$,

$$\left| \bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}} + \langle \mathbf{g}_1, \cdots, \mathbf{g}_{i-1} \rangle \right| \tag{5.23}$$

$$\leq | \bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}} | q^{i-1} \tag{5.24}$$

$$\leq \binom{|\mathcal{E}|}{n-k} q^{n-k} q^{i-1} \tag{5.25}$$

$$= \binom{|\mathcal{E}|}{n-k} q^{n-k+i-1} \tag{5.26}$$

$$\leq \binom{|\mathcal{E}|}{n-k} q^{n-1} \tag{5.27}$$

which does not depend on i.

If

$$q > \binom{|\mathcal{E}|}{n-k}, \tag{5.28}$$

then there exists a vector that can be chosen as $\mathbf{g}_i$ for $i = 1, \cdots, k$. Note that by virtue of (5.22), $\mathbf{g}_i \neq 0$ for all i.

Fix $\mathbf{g}_1, \cdots, \mathbf{g}_k$ that satisfy (5.22). We prove by induction that

$$\left(\bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}} \right) \cap \langle \mathbf{g}_1, \cdots, \mathbf{g}_i \rangle = \{0\}. \tag{5.29}$$

holds for these $\mathbf{g}_i$. If (5.29) does not hold for $i = 1$, then there exists a non-zero vector $\alpha \mathbf{g}_1 \in \bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}}$, where $\alpha \in \mathbb{F} \backslash \{0\}$. Since $\bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}}$ is closed under scalar multiplication and $\alpha \neq 0$, we have $\mathbf{g}_1 \in \bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}}$, a contradiction to (5.22) for $i = 1$. Assume (5.29) holds for $i \leq k-1$. If (5.29) does not hold for $i = k$, then there exists a non-zero vector

$$\sum_{i=1}^{k} \alpha_i \mathbf{g}_i \in \bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}}, \tag{5.30}$$

where $\alpha_i \in \mathbb{F}_q$. If $\alpha_k = 0$, then

$$\sum_{i=1}^{k-1} \alpha_i \mathbf{g}_i \in \bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}}, \tag{5.31}$$

a contradiction to the assumption that (5.29) holds for $i = k-1$. Thus $\alpha_k \neq 0$. Again, by $\bigcup_{\mathrm{W} \in \mathcal{W}'} \mathcal{L}_{\mathrm{W}}$ being closed under scalar multiplication, we have

$$\begin{aligned} \mathbf{g}_k &\in \bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}} - \left\{ \alpha_k^{-1} \sum_{i=1}^{k-1} \alpha_i \mathbf{g}_i \right\} && (5.32) \\ &\subset \bigcup_{\mathrm{W}\in\mathcal{W}'} \mathcal{L}_{\mathrm{W}} + \langle \mathbf{g}_1, \cdots, \mathbf{g}_{k-1} \rangle, && (5.33) \end{aligned}$$

a contradiction to (5.22) for $i = k$. Therefore, $\mathbf{g}_1, \cdots, \mathbf{g}_k$ satisfy (5.29) and we let $\mathcal{C} = \langle \mathbf{g}_1, \cdots, \mathbf{g}_k \rangle$.

For any subspace D of $\mathcal{C}$. For any $\mathrm{W} \subset \mathcal{E}$ with $|\mathrm{W}| \leq n - k$, it follows from (5.29) for $i = k$ that

$$\mathcal{L}_{\mathrm{W}} \cap D = \{0\}. \tag{5.34}$$

In particular, (5.34) holds when the dimension of D is equal to 1. Therefore, by Definition 5.2, $w_{\min} = d_1(\mathcal{C}, F) \geq n - k + 1$. Together with Theorem 5.2, we obtain

$$w_{\min} = n - k + 1 \tag{5.35}$$

The proof is completed. □

Theorem 5.4. *Given an $[n, k]$ linear code $\mathcal{C}$ with $|\mathcal{C}| = q^k$, we can construct a linear multicast over a finite field $\mathbb{F}$, when q is sufficiently large, such that*

$$w_{\min} = n - k + 1 \tag{5.36}$$

Proof. We first use Jaggi-Sanders' algorithm in [11] to construct an n-dimensional deterministic linear multicast, whose global encoding kernels are denoted by $F' = \{f'_e, e \in \mathcal{E}\}$. Then we use the method in the proof of Theorem 5.3 to find an $[n,k]$ linear code $\mathcal{C}'$ that achieves the upper bound in (5.19), i.e., $d_1(\mathcal{C}', F') = n - k + 1$. We will show that $\mathcal{C}$ can be obtained from $\mathcal{C}'$ by taking an invertible linear transformation T, i.e., $T(c') = c'M, \forall c' \in \mathcal{C}'$, where M is an $n \times n$ invertible matrix. Let $f_e = M^{-1}f'_e$ for $e \in \mathcal{E}$. We will further show that the set of global encoding kernel $F = \{f_e : e \in \mathcal{E}\}$ achieves the upper bound in (5.19).

i) Let G_0 be a $k \times n$ matrix formed by the first k rows of the $n \times n$ identity matrix I, and G and G' be the generator matrix of $\mathcal{C}$ and $\mathcal{C}'$, respectively. We form two invertible $n \times n$ matrices M_1 and M_2, such that the first k columns of M_1 and M_2 are G^T and G'^T respectively. Then $G_0 M_1^T = G$ and $G_0 M_2^T = G'$. Hence $G(M_2 M_1^{-1})^T = G'$ and M can be taken to be $M_2 M_1^{-1}$.

ii) The sink nodes in the network can still decode successfully with the new network code specified by the global encoding kernels $\{f_e : e \in \mathcal{E}\}$ since M is invertible. We now prove that the linear code $\mathcal{C}$ achieves the upper bound in (5.19) with respect to $F = \{f_e : e \in \mathcal{E}\}$. Assume that $\mathcal{C}$ does not achieve the upper bound, i.e., $w_{\min} = d_1(\mathcal{C}, F) \leq n - k$ or $k < n - w_{\min} + 1$. Then according to the definition of the generalized Hamming weight, $\exists \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq 0$ and $n - k$ global encoding kernels, say $f_1, f_2, \cdots, f_{n-k}$, such that $\mathbf{c} = a_1 f_1^T + \cdots + a_{n-k} f_{n-k}^T$ and $a_i, i = 1 \cdots n - k$ are not all zero.

Therefore,

$$\mathbf{c} = (a_1 f_1'^T + a_2 f_2'^T + \cdots + a_{n-k} f_{n-k}'^T)(M^T)^{-1} \tag{5.37}$$

or

$$\mathbf{c}M^T = a_1 f_1'^T + a_2 f_2'^T + \cdots + a_{n-k} f_{n-k}'^T. \tag{5.38}$$

Let $c' = cM^{-1}$. Since $\langle c' \rangle$ is a 1-dimensional subcode of $\mathcal{C}'$, in light of (5.38) and Definition 5.2, $d_1(\mathcal{C}', F')$ is less than $n-k+1$. This is contradictory to that $\mathcal{C}'$ achieves the upper bound in (5.19).

The proof is completed. □

Theorem 5.5. *Given a linear code $\mathcal{C}$ (a linear multicast specified by $F = \{f_e, e \in \mathcal{E}\}$), we can find a corresponding linear multicast specified by $F = \{f_e, e \in \mathcal{E}\}$(linear code $\mathcal{C}$), such that the tightness of the generalized Singleton bound of $\mathcal{C}$ can be achieved, that is, $d_r(\mathcal{C}, F) = n-k+r, \forall 1 \leq r \leq k$.*

Proof. $d_1(\mathcal{C}, F) = n-k+1$ is obtained by the Theorem 5.3 (Theorem 5.4). Together with the monotonicity property obtained in Lemma 5.1 and the fact that $d_k(\mathcal{C}, F) \leq n$, we can see that $d_r(\mathcal{C}, F) = n-k+r, \forall 1 \leq r \leq k$ are also obtained automatically. □

5.2.2 Network MDS Code

Here we introduce the term *Network Maximum Distance Separable* (*NMDS*) code to identify those linear codes that can be used to achieve the generalized Singleton bound based on a given linear network code. Such a name is given to these linear codes is motivated by the fact that in the classical channel, MDS code is the only linear code that can achieve the generalized Singleton bound induced by the generalized Hamming weight.

Definition 5.3. *Given a full-rank linear network code, a* Network Maximum Distance Separable *code (*NMDS*) is a linear block code that achieves the tightness of the generalized Singleton bound.*

By Theorem 5.4, for any full-rank block code, we can find a corresponding full-rank linear network code such that the generalized Singleton bound is achieved. In other words, any full-rank block code is an NMDS code for some full-rank linear network code. However, such a block code is not necessarily an MDS code.

On the other hand, with respect to the full-rank network code depicted in Figure 5.1, a linear block code is an NMDS code if and only if it is an MDS code.

5.3 Application of Network Generalized Hamming Weight

The generalized Hamming weight in [9] can completely characterize the performance of a linear code $\mathcal{C}$ on the wiretap channel II. Our definition of network generalized Hamming weight can also fully characterize the performance of a linear code $\mathcal{C}$ on the CSWN, which can be treated as a network generalization of wiretap channel II.

The problem of secure network coding was first studied by Cai and Yeung in [5]. They introduced the CSWN, which subsumes the secret-sharing model proposed independently by Blakley [14] and Shamir [15], and proposed a secure network coding scheme. A CSWN consists of a network and a collection $\mathcal{W}$ of subsets of channels, whose members are called wiretap subsets of channels. An eavesdropper can arbitrarily choose one but only one wiretap subset $\mathrm{W} \in \mathcal{W}$ and fully access (the output of) all the channels in the wiretap subset W. The communicators over a CSWN know the collection $\mathcal{W}$ of wiretap subsets but do not know which subset W is chosen by the eavesdropper. The goal of the communicators is that the eavesdropper can obtain absolutely no information about the messages transmitted through the network. Such secure network codes have been further studied in [12] by Feldman et al. Later on, Cai and Yeung continued their original work in [6] with a more general model in which there are more than one source node and randomness can be generated at an arbitrarily given subset of nodes, and obtained a necessary and sufficient condition for the security of a network code. In their latest work [13], they further prove for the special case that the eavesdropper may choose to access any subset of channels of a fixed size, the code they constructed in [5] achieves the required security with the minimum amount of randomness and at the same time multicasts the maximum possible amount of information.

In this chapter, we assume that there is an eavesdropper in the network who can arbitrarily choose and fully access μ edges of the network. We define $\mathcal{W} := \{\mathrm{W} \subset \mathcal{E} : |\mathrm{W}| = \mu\}$ and say an eavesdropper is characterized by $\mathcal{W}$ if the eavesdropper can arbitrarily choose and access one and only one set in $\mathcal{W}$.

We denote the message that the source node wants to transmit securely by a k-dimensional row vector $\mathbf{s} \in \mathbb{F}_q^k$ and let $\mathcal{C}$ be an $[n, n-k]$ linear code and $\mathbf{H}$ be the $k \times n$ parity check matrix of $\mathcal{C}$. In order to protect the messages from the eavesdropper, we apply coset coding [8] based on $\mathcal{C}$ at the source node as follows: The encoded message that is transmitted in the network is denoted by an n-dimensional row vector

$\mathbf{x} \in \mathbb{F}_q^n$. The source selects one of the q^k cosets to represent $\mathbf{s}$, and transmits a vector $\mathbf{x}$ chosen from that coset according to the uniform distribution. Equivalently, we can write

$$\mathbf{x} = [\ \mathbf{s} \ \ \mathbf{r}\ ] \begin{bmatrix} G_M \\ G_C \end{bmatrix}, \tag{5.39}$$

where G_C is the $(n-k) \times n$ generator matrix of $\mathcal{C}$, G_M is any $k \times n$ full-rank matrix such that G_M and G_C together forms a $n \times n$ full-rank matrix, and $\mathbf{r}$ is chosen from $|\mathbb{F}_q^{n-k}|$ uniformly. See Appendix A for a proof.

Let S be the random variable denoting the information source, X be the random variable denoting the source of the encoded message to be transmitted by the source node, and Y be the random variable denoting the message received by the eavesdropper.

We denote the symbols that the eavesdropper obtains by a |W|-dimensional row vector $\mathbf{y} \in \mathbb{F}_q^{|\mathrm{W}|}$. Write $\mathbf{s} = (s_1, s_2, \cdots, s_k), \mathbf{x} = (x_1, x_2, \cdots, x_n)$ and $\mathbf{y} = (y_1, y_2, \cdots, y_{|\mathrm{W}|})$. The symbols in $\mathbf{s}$ and $\mathbf{x}$ are i.i.d. and chosen uniformly from $\mathbb{F}_q$. Since G_M and G_C together form an $n \times n$ full-rank matrix, $\forall \mathbf{s} \in \mathbb{F}_q^k$ s.t. $\mathbf{s} \neq 0, \mathbf{s}G_M\mathbf{H}^T \neq 0$, otherwise, there exists a non-zero vector $R \in \mathbb{F}_q^{n-k}$ such that $\mathbf{s}G_M = \mathbf{r}G_C$. This contradicts the fact that G_M and G_R together forms a $n \times n$ full-rank matrix. Therefore, $G_M\mathbf{H}^T$ is invertible. Then letting $\mathbf{H}' = (G_M\mathbf{H}^T)^{-1}$, we have

$$\begin{aligned}\mathbf{x}\mathbf{H}^T\mathbf{H}' =& [\,\mathbf{s}\ \ \mathbf{r}\,]\begin{bmatrix} G_M \\ G_C \end{bmatrix}\mathbf{H}^T\mathbf{H}' && (5.40)\\ =& \mathbf{s}G_M\mathbf{H}^T\mathbf{H}' && (5.41)\\ =& \mathbf{s}, && (5.42)\end{aligned}$$

giving the formula for recovering the information source $\mathbf{s}$ from the encoded message $\mathbf{x}$.

We assume that the eavesdropper knows the $[n, n-k]$ linear code $\mathcal{C}$ and its parity check matrix $\mathbf{H}$ used in the coset coding scheme as well as the matrix $F_{\mathcal{E}}$. We define the uncertainty of the eavesdropper about the source as $\Delta = \min_{\mathrm{W}\in\mathcal{W}} H(S|Y)$, and say the network is perfectly secured if $\Delta = H(S) = k$. Here $H(\cdot)$ denotes entropy in the base q, and conditional entropy will be denoted by $H(\cdot|\cdot)$.

In another independent work [7], Rouayheb and Soljanin treated the single source secure network coding problem as a network generalization of the Ozarow-Wyner's wiretap channel II in [8], and gave an secure construction method based on coset coding, which was equivalent to the approach in [5] with the exception that the authors in [8] assumed the linear block code at the source node must be an MDS code.

Theorem 5.6. *Given an acyclic directed network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$, a linear multicast (see Definition 1.5), and an eavesdropper characterized by $\mathcal{W} = \{W \subset \mathcal{E} : |W| \leq \mu\}$, if we apply coset coding at the source node using an $[n, n-k]$ linear code $\mathcal{C}$, then*

i) the eavesdropper cannot obtain any information about the source, *i.e., $\Delta = k$, if and only if $d_1(\mathcal{C}^\perp, F) > \mu$.*

ii) the eavesdropper can obtain r units of information about the source, i.e., $\Delta = k - r$, if and only if $\mu \geq d_r(\mathcal{C}^\perp, F)$.

Proof. We first compute the uncertainty of the eavesdropper about the source. Let $\mathbf{H}$ be the parity check matrix of $\mathcal{C}$. Then $(\mathbf{H}')^T\mathbf{H}\mathbf{x}^T = \mathbf{s}^T$ according to (5.42) and $\mathbf{x}F_{\mathrm{W}} = \mathbf{y}$.

$$\Delta = \min_{\mathrm{W}\in\mathcal{W}} H(S|Y) \tag{5.43}$$

$$= \min_{\mathrm{W}\in\mathcal{W}} \left\{H(S|X,Y) + H(X|Y) - H(X|S,Y)\right\}. \tag{5.44}$$

$$\begin{cases} \mathbf{H}'^T\mathbf{H}\mathbf{x}^T = \mathbf{s}^T \\ F_{\mathrm{W}}^T\mathbf{x}^T = \mathbf{y}^T \end{cases} \tag{5.45}$$

$$\Rightarrow \quad \begin{bmatrix} \mathbf{H}'^T\mathbf{H} \\ F_{\mathrm{W}}^T \end{bmatrix}\mathbf{x}^T = \begin{bmatrix} \mathbf{s}^T \\ \mathbf{y}^T \end{bmatrix} \tag{5.46}$$

The dimension of solution space of (5.46) is $n - rank\left(\begin{bmatrix} \mathbf{H}'^T\mathbf{H} \\ F_{\mathrm{W}}^T \end{bmatrix}\right)$.

Since we assumed $\mathbf{x}$ is uniformly distributed,

$$H(X|S,Y) = n - rank\left(\begin{bmatrix} \mathbf{H}'^T\mathbf{H} \\ F_{\mathrm{W}}^T \end{bmatrix}\right) \tag{5.47}$$

$$= n - rank(\mathbf{H}'^T\mathbf{H}) - rank(F_{\mathrm{W}}^T) + \dim\left(\mathcal{C}^\perp \cap \mathcal{L}_{\mathrm{W}}\right) \tag{5.48}$$

$$= n - k - rank(F_{\mathrm{W}}^T) + \dim\left(\mathcal{C}^\perp \cap \mathcal{L}_{\mathrm{W}}\right), \tag{5.49}$$

where (5.48) comes from the fact $\mathbf{H}'$ is a full-rank matrix and (5.49) comes from (5.42), and $H(S|X,Y) = 0$, $H(X|Y) = n - rank(F_{\mathrm{W}})$, thus

$$\Delta = k - \max_{\mathrm{W} \in \mathcal{W}} \dim\left(\mathcal{C}^{\perp} \cap \mathcal{L}_{\mathrm{W}}\right). \tag{5.50}$$

From (5.50), the proof for i) and ii) follows immediately:

i) $d_1(\mathcal{C}^{\perp}, F) > \mu$, i.e., $\forall \mathrm{W} \in \mathcal{W}$, $\dim\left(\mathcal{C}^{\perp} \cap \mathcal{L}_{\mathrm{W}}\right) = 0$, is equivalent to $\Delta = k$.

ii) $\mu \geq d_r(\mathcal{C}^{\perp}, F)$, i.e., $\exists \mathrm{W} \in \mathcal{W}$ s.t. $\dim\left(\mathcal{C}^{\perp} \cap \mathcal{L}_{\mathrm{W}}\right) = r$, is equivalent to $\Delta \leq k - r$.

□

In other words, similar to the role of the original definition of generalized Hamming weight [9] for the classical point-to-point channel, our definition of generalized Hamming weight can also be used to measure the security performance of a linear code $\mathcal{C}$ for a given linear network code on a given network.

5.3.1 Optimality of NMDS Code

We will see that applying coset coding using a code $\mathcal{C}$ whose dual is an NMDS code is in fact a linear network code with optimal security performance. The following theorem gives a lower bound on the information of the source that the eavesdropper can obtain despite the coding scheme being used to multicast information.

Theorem 5.7. *Given an acyclic directed network* $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ *with maxflow n, and a linear multicast transmitting information at rate k* *from the source node s to the set of sink nodes $\mathcal{T}$, the information that the eavesdropper, who can wiretap any set of τ channels, where $n-k \leq \tau \leq n$, can obtain at least $k+\tau-n$ units of information.*

Proof. See Appendix B. □

By Definition 5.3, NMDS code achieves the tightness of the generalized Singleton bound, i.e.,

$$d_r(\mathcal{C}^\perp, F) = n - k + r. \tag{5.51}$$

Let r' be the maximum number of information the eavesdropper can get by wiretapping τ channels. Then by ii) of Theorem 5.6,

$$\tau \geq d'_r(\mathcal{C}^\perp, F) = n - k + r' \tag{5.52}$$

$$\Rightarrow r' \leq k + \tau - n. \tag{5.53}$$

Therefore, the maximum amount of information that the eavesdropper can obtain is $k+\tau-n$ which is also minimal according to Theorem 5.7. Therefore, we can see that applying coset coding using a code $\mathcal{C}$ whose dual is an NMDS code is in fact constructing a linear network code which can guarantee that the information obtained by the eavesdropper is minimal, that is, the security performance of the overall linear network code is optimal.

According to the result by Wei [9], if we apply coset coding based on $[n, n-k]$ linear code $\mathcal{C}$ in wiretap channel II problem, the eavesdropper who can access at most $(n-k)$ channels gains no information about the source (we say the system achieves the best security performance) if and only if the dual code of $\mathcal{C}$ is an MDS code. In our problem, the network achieves the best security performance if and only if the dual code of $\mathcal{C}$ is an NMDS code.

Corollary 5.2. *Given an acyclic directed network $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ and a linear multicast achieving the maxflow bound n, if we apply coset coding at the source based on an $[n, n-k]$ linear code $\mathcal{C}$, such that $\mathcal{C}^{\perp}$ is an NMDS code, then the network is perfectly secure against any eavesdropper with $\mathcal{W}' = \{W \subset \mathcal{E} : |W| \leq n-k\}$ while information can be multicast to the sink nodes at the rate of k.*

In [7], Rouayheb and Soljanin gave a coding scheme, which is a construction of linear secure network code based on MDS code. In fact, according to our analysis of NMDS code, we can construct linear secure network code based on any full-rank linear block code.

5.3.2 Examples

We consider the kind of degenerated network in which there are only one source node and one sink node. The source node is connected directly to the sink node with 7 channels. Let the global encoding kernels of the channels be $\delta_i, 1 \leq i \leq 7$, respectively, where δ_i is the unit 7-dimensional column vector whose components are all equal zero except that the *ith* component is equal to 1. Such a network and the corresponding global encoding kernel are indicated in Figure 5.2. Now, we are going to measure the security performance of a given linear code

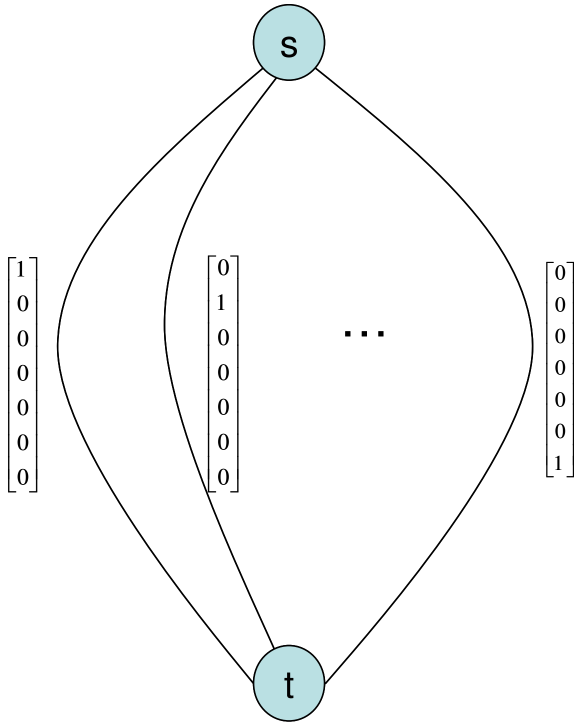


Figure 5.2: A degenerated network.

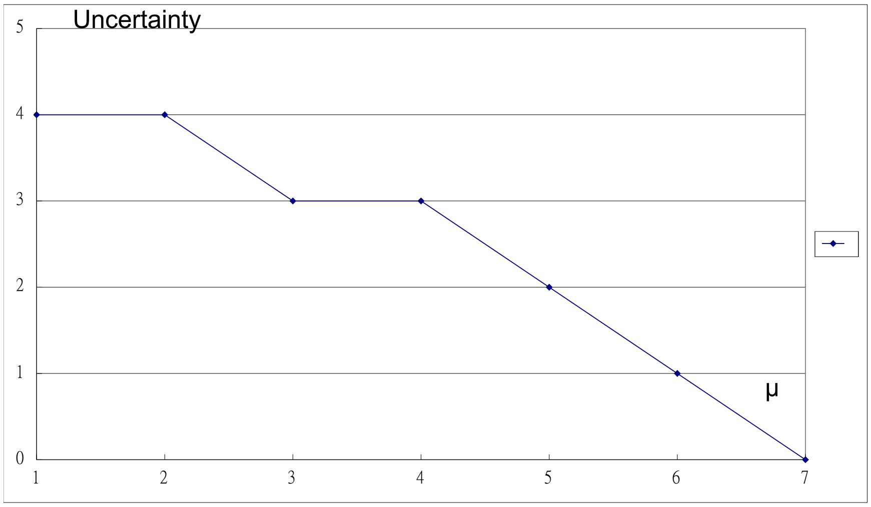


Figure 5.3: Security curve of code $\mathcal{C}_1$ with respect to Figure 5.2.

$\mathcal{C}_1$. Let the generator matrix $\mathbf{G}_1$ of a linear code $\mathcal{C}_1$ be

$$\mathbf{G}_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 2 & 3 \\ 0 & 1 & 0 & 1 & 2 & 4 & 1 \\ 0 & 0 & 1 & 1 & 3 & 3 & 6 \end{bmatrix}. \tag{5.54}$$

With the given generator matrix and global encoding kernel, we can then show that

$$d_1(\mathcal{C}_1^{\perp}, F) = 3, \tag{5.55}$$

$$d_2(\mathcal{C}_1^{\perp}, F) = 5, \tag{5.56}$$

$$d_3(\mathcal{C}_1^{\perp}, F) = 6 \tag{5.57}$$

and

$$d_4(\mathcal{C}_1^{\perp}, F) = 7 \tag{5.58}$$

where $F = \{\delta_i, 1 \leq i \leq 7\}$.

The dual of $\mathcal{C}$, a [7,4] code, is used as the linear block code at the source node. Then, by the result in Theorem 5.6, we can see that the adversary cannot gain any useful information by eavesdropping just 1 or 2 channels in the network. We can see there is a drop in the uncertainty of the adversary about the source information when it can gain access to set of 3 channels in the network. However, when the adversary can gain access to an extra channel in the network, i.e. totally 4 channels, the unit of useful information that the adversary can resolve is still equal to 1. That is, accessibility to one extra channel does not give the adversary any additional benefit if it can already access 3 channels in

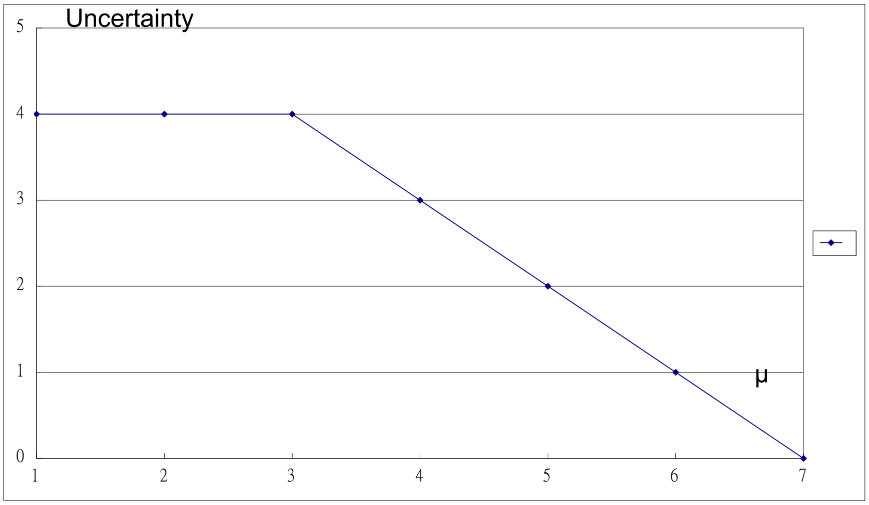


Figure 5.4: Security curve of code $\mathcal{C}_2$ with respect to Figure 5.2.

the network. However, as indicated in Figure 5.3, when the adversary can gain access to 5, 6 and 7 channels in the network, the amount of source information that the adversary can obtain will be 2, 3 and 4 respectively.

From this example, we can see that the generalized Hamming weights of the dual code in fact characterize the drops of the security curve.

Next, we will show that a different linear code $\mathcal{C}$ at the source node that will give an optimal security performance for the overall transmission with the same given network and linear network code. Given the same network and linear network code as indicated in Figure 5.2, we now let the generator matrix $\mathbf{G}_2$ of a linear code $\mathcal{C}_2$ to be

$$\mathbf{G}_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 2 & 3 \\ 0 & 1 & 0 & 1 & 2 & 5 & 1 \\ 0 & 0 & 1 & 1 & 3 & 3 & 6 \end{bmatrix}. \tag{5.59}$$

With the given generator matrix and global encoding kernels, we can then show that

$$d_1(\mathcal{C}_2^{\perp}, F) = 4, \tag{5.60}$$

$$d_2(\mathcal{C}_2^{\perp}, F) = 5, \tag{5.61}$$

$$d_3(\mathcal{C}_2^{\perp}, F) = 6 \tag{5.62}$$

and

$$d_4(\mathcal{C}_2^{\perp}, F) = 7. \tag{5.63}$$

as indicated in Figure 5.4.

By the generalized Singleton bound in Theorem 5.2, we can see that the overall security performance is already optimal. According to the definition of Network MDS code in Section 5.2.2, the dual code of $\mathcal{C}_2$ is an NMDS code with respect to the given linear network code on the given network.

On the other hand, the linear code $\mathcal{C}_1$ is not a network MDS code with respect to the given linear network code on the given network as indicated in Figure 5.2. However, it worth noting that an NMDS code with respect to a given linear network code does not necessarily imply that it is an NMDS code with respect to another linear network code.

Figure 5.5 indicates the same degenerated network discussed previously but with a different set of global encoding kernels. With the same linear network code $\mathcal{C}_2$, the generalized Hamming weights become

$$d_1(\mathcal{C}_2^{\perp}, F) = 2, \tag{5.64}$$

$$d_2(\mathcal{C}_2^{\perp}, F) = 5, \tag{5.65}$$

$$d_3(\mathcal{C}_2^{\perp}, F) = 6 \tag{5.66}$$

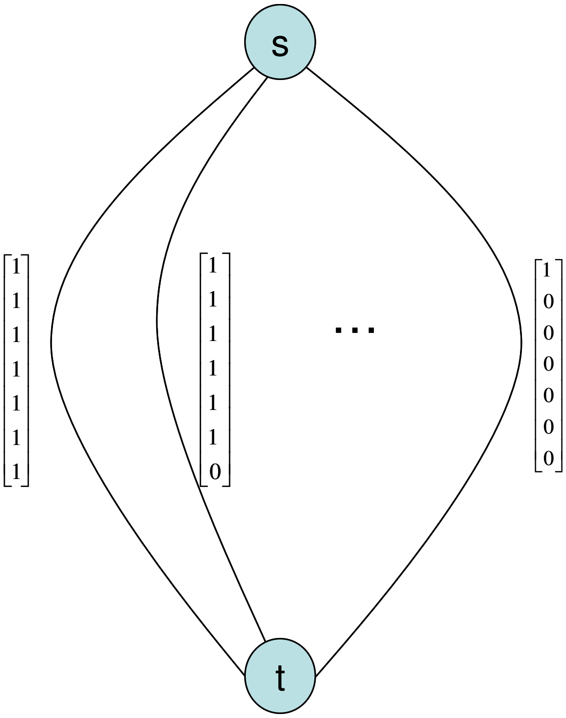


Figure 5.5: A degenerated network with different global encoding kernels.

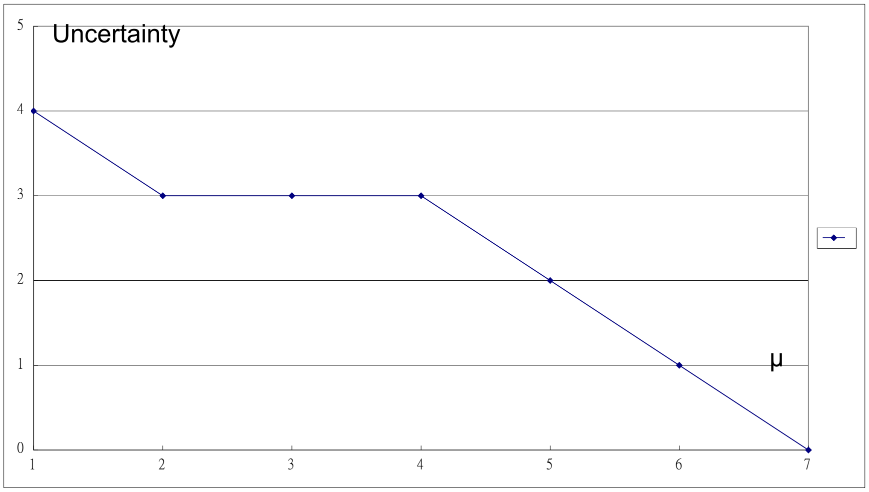


Figure 5.6: Security curve of code $\mathcal{C}_2$ with respect to Figure 5.5.

and

$$d_4(\mathcal{C}_2^{\perp}, F) = 7. \tag{5.67}$$

as indicated in Figure 5.6 where

$$F = \left\{ \begin{bmatrix}1\\1\\1\\1\\1\\1\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\\1\\1\\1\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\\1\\1\\0\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\\1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\1\\1\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\1\\0\\0\\0\\0\\0\end{bmatrix}, \begin{bmatrix}1\\0\\0\\0\\0\\0\\0\end{bmatrix} \right\}. \tag{5.68}$$

Since the linear code cannot obtain the best security performance on the given network with the given linear network code, it is not a Network MDS code in this case.

5.4 One-Pass Construction of Secure Network Code

In this section, we present an algorithm for constructing a secure network code achieving the generalized Singleton bound. The main difference between this construction and those have been discussed previously is that it is a one-pass algorithm in the sense that the linear code $\mathcal{C}$ and the global encoding kernels will be chosen in an upstream-to-downstream manner. Once the linear block code $\mathcal{C}$ and the global encoding kernels have been fixed, they do not need to be changed.

Algorithm (One-Pass Construction for Secure Network Code)

Let $\{t_1, t_2, \ldots, t_\delta\}$ be the set of sink nodes in the acyclic network with $maxflow(t_q) \geq n, \forall 1 \leq q \leq \delta$. This algorithm constructs a linear block code and an n-dimensional $\mathbb{F}$-valued linear network code, where $\mathbb{F}$ is the finite field on which the code is defined, that together can multicast data securely at the rate $n - k$ to all the predefined sink nodes on the acyclic network with the presence of adversary that can eavesdrop any set of k channels in the network. We are going to show that such an algorithm always exists when

$$|\mathbb{F}| > \delta + \left(\begin{array}{c} |\mathcal{E}| \\ k-1 \end{array} \right). \tag{5.69}$$

Let a pair of channels (e_i, e_j) be called an adjacent pair when there exists a node $t \in \mathcal{V}$ with $e_i \in In(t)$ and $e_j \in Out(t)$. A sequence of channels $e_1, e_2, ..., e_l$ is called a path from a node u to a node v when $e_1 \in Out(u), e_l \in In(v)$, and (e_j, e_{j+1}) is an adjacent pair for all j. For each $q, 1 \leq q \leq \delta$, there exist channel-disjoint paths $P_{q,1}, P_{q,2}, ..., P_{q,n}$ from s to t_q. Altogether there are δn paths. Adopt the notation $V_t = \langle \{f_e : e \in In(t)\} \rangle$ where f_e denotes the global encoding kernel of edge e and $\langle \cdot \rangle$ is the conventional notation for the linear span of a set of vectors. We first choose and fix an $[n, n-k]$ linear code $\mathcal{C}$. The following procedure will then prescribe a global encoding kernel f_e for every channel e in the network such that $dim(V_{t_q}) = n$ for $1 \leq q \leq \delta$ while maintaining the secrecy of the data transmitted.

```
{
    // By definition, the global encoding kernels for the $n$
    // imaginary channels [10] of the source node $s$ form
    // the standard basis of $\mathbb{F}^n$
for (every channel $e$ in the network)
$f_e$ = the zero vector;
    //This is just initialization. $f_e$ will be updated in an
    //upstream-to-downstream order.
```

```
for ($q = 1; q \leq \delta; q++$)
    for ($i = 1; i \leq n; i++$)
    {
    $e_{q,i}$ = the imaginary channel initiating the path
        $P_{q,i}$;
    //This is just initialization. Later $e_{q,i}$ will be
    //dynamically updated by moving down along the
    //path $P_{q,i}$ until finally $e_{q,i}$ becomes a channel in
    //$In(t_q)$.
    }

for (every node $t$, in any upstream-to-downstream order)
{
for (every channel $e \in Out(t)$)
{
    //With respect to this channel $e$, define a “pair” as a
    //pair $(q, i)$ of indices such that the channel $e$ is
    //on the path $P_{q,i}$. Note that for each $q$, there
    //exists at most one pair $(q, i)$. Thus, the number
    //of pairs is at least 0 and at most $\delta$.
    //Since the nodes $t$ are chosen in an
    //upstream-to-downstream manner, if $(q, i)$ is a
    //pair, then $e_{q,i} \in In(t)$ by induction, so that
    //$f_{e_{q,i}} \in V_t$. For reasons to be explained in the
    //justification below, $f_{e_{q,i}} \notin \langle\{f_{e_{q,i}} : j \neq i\}\rangle$.
Choose a vector $w$ in $V_t$ such that $w \notin \langle\{f_{e_{q,j}} : j \neq i\}\rangle$ for every pair
$(q, i)$ and $\langle\{w\} \cup \{f_i, i \in K\}\rangle \cap \mathcal{C}^{\perp} = \emptyset, \forall K \subset \mathcal{E}, |K| = k - 1$;
```

```
        //For the sake of clarity, the existence
        //of such vector $w$ will be justified right
        //after the algorithm.
    $f_e = w$
        //This is equivalent to choosing scalar values for
        //local encoding kernels $k_{d,e}$ for all $d \in In(t)$
        //such that $\sum_{d\in In(t)} k_{d,e} f_d \notin \left\langle \{f_{e_{q,j}}\} \right\rangle$ for
        //every pair $(q,i)$ while maintaining the
        //maximum security condition.
    For (every pair $(q,i)$)
    $e_{q,i} = e$;
        }
      }
    }
```

To see the existence of such a vector w, denote $dim(V_t) = k$. Then, $dim\left(V_t \cap \left\langle \{f_{e_{q,j}} : j \neq i\} \right\rangle\right) \leq k-1$ for every pair (q,i) since $f_{e_{q,i}} \in V_t \backslash \left\langle \{f_{e_{q,j}} : j \neq i\} \right\rangle$. Thus $\left|V_t \cap (\cup_{(q,i)\text{a pair}} \left\langle \{f_{e_{q,j}} : j \neq i\} \right\rangle)\right| \leq \delta |\mathbb{F}|^{k-1}$.

Since $\forall K \subset \mathcal{E}, |K| = k-1, \left\langle \{f_{e_{q,i}}\} \cup \{f_i, i \in K\} \right\rangle \cap \mathcal{C}^{\perp} = \emptyset$, then

$$\begin{aligned} & dim(\langle V_t \cup \{f_i, i \in K\} \rangle \cap \mathcal{C}^{\perp}) \\ \leq & k-1. \end{aligned} \tag{5.70}$$

Thus

$$\begin{aligned} & \left|\cup_{K \subset \mathcal{E}, |K| = k-1} \left(\langle V_t \cup \{f_i, i \in K\} \rangle \cap \mathcal{C}^{\perp}\right)\right| \\ \leq & \begin{pmatrix} |\mathcal{E}| \\ k-1 \end{pmatrix} |\mathbb{F}|^{k-1}. \end{aligned} \tag{5.71}$$

Justification. For $1 \leq q \leq \delta$ and $1 \leq i \leq n$, the channel $e_{q,i}$ is on the path $P_{q,i}$. Initially $e_{q,i}$ is an imaginary channel at s. Through dynamic updating it moves downstream along the path until finally reaching a channel in $In(t_q)$.

Fix an index q, $1 \leq q \leq \delta$. Initially, the vectors $f_{e_{q,1}}, f_{e_{q,2}}, \ldots, f_{e_{q,n}}$ are linearly independent because they form the standard basis of $\mathbb{F}^n$. At the end, in order for the eventually constructed linear network code to qualify as secure linear multicast, it suffices to show the preservation of the linear independence among $f_{e_{q,1}}, f_{e_{q,2}}, \ldots, f_{e_{q,n}}$ and that they satisfy the condition of secure network code throughout the algorithm.

Fix a node t and a channel $e \in Out(t)$. We need to show the preservation in the generic step of the algorithm for each channel e in the "for loop." The algorithm defines a "pair" as a pair (q, i) of indices such that the channels e is on the path $P_{q,i}$. When no (q, i) is a pair for $1 \leq i \leq n$, the channels $e_{q,1}, e_{q,2}, \ldots, e_{q,n}$ are not changed in the generic step; neither are the vectors $f_{e_{q,1}}, f_{e_{q,2}}, \ldots, f_{e_{q,n}}$. So we may assume the existence of a pair (q, i) for some i. The only change among the channels $e_{q,1}, e_{q,2}, \ldots, e_{q,n}$ is that $e_{q,i}$ becomes e. Meanwhile, the only change among the vectors $f_{e_{q,1}}, f_{e_{q,2}}, \ldots, f_{e_{q,n}}$ is that $f_{e_{q,i}}$ becomes a vector $w \notin \langle \{f_{e_{q,j}} : j \neq i\} \rangle$ and $\langle \{w\} \cup \{f_i, i \in K\} \rangle \cap \mathcal{C}^{\perp} = \emptyset, \forall K \subset \mathcal{E}, |K| = k-1$. This preserves the linear independence among $f_{e_{q,1}}, f_{e_{q,2}}, \ldots, f_{e_{q,n}}$ and the secure condition of a secure linear network code as desired.

Analysis of complexity. Let N be the number of channels in the network as in the algorithm. For each channel e, the "for loop" in the Algorithm process at most $\begin{pmatrix} N \\ k-1 \end{pmatrix}$ collections of $k-1$ channels plus δ pairs.

The processing includes the calculation of the set

$$V_t \backslash \left(\cup_K \left(\langle V_t \cup \{f_i, i \in K\} \rangle \cap \mathcal{C}^{\perp} \right) \right. \\ \left. \cup \left(\cup_{\text{a pair}} \left\langle \{ f_{e_{q,j}} : j \neq i \} \right\rangle \right) \right). \tag{5.72}$$

This can be done by, for instance, Gaussian elimination.

Throughout the algorithm, the total number of collections of $k-1$ channels and pairs processed is at most $N\left(\left(\begin{array}{c} N \\ k-1 \end{array}\right)+\delta\right)$, a polynomial in N of degree n. Thus, for a fixed n, it is not hard to implement the algorithm with a polynomial time in N.

5.5 Reduction to the Classical Communication Channel

In this section, we show that our new definition of generalized Hamming weight reduces to the generalized Hamming weight proposed in [9] when the network being considered is the degenerated network representing the classical communication channel. In such a network, there are only one source node and one sink node. The source node is connected directly to the sink node with n channels. Let the global encoding kernels of the channels be $\delta_i, 1 \leq i \leq n$, respectively, where δ_i is the unit n-dimensional column vector whose components are all equal to zero except that the ith component is equal to 1.

According to our definition,

$$\begin{aligned} d_r(\mathcal{C}, F) = \min \big\{ |\mathrm{W}| : \big\langle \big\{ \delta_i^T, i \in \mathrm{W} \big\} \big\rangle & \text{ contains} \\ \text{some subcode } D \text{ of } \mathcal{C} & \text{ with dimension } r \big\} \end{aligned} \tag{5.73}$$

where $F = \{\delta_i, 1 \le i \le n\}$.

Next, we will show that (5.73) is equivalence to the definition of generalized hamming weight for the classical point-to-point channel.

The support of a subcode D of C, denoted $\mathcal{X}(D)$, is the set of not-always-zero element positions of D, that is,

$$\mathcal{X}(C) \triangleq \{i : \exists (x_1, x_2, \ldots, x_n) \in C, x_i \neq 0\}. \tag{5.74}$$

Definition 5.4. *(Generalized Hamming Weight [9])*

$$d'_r(\mathcal{C}) \triangleq \min\{|\mathcal{X}(D)| : D \textit{ is a subcode of } C \textit{ with dimension } r\}. \tag{5.75}$$

Let D be a subcode of C with dimension r such that $|\mathcal{X}(D)| = d'_r(\mathcal{C})$. Without loss of generality, assume $\mathcal{X}(D) = \{1, 2, \ldots, d'_r(\mathcal{C})\}$. This implies that $\forall \mathbf{x} \in D, x_i = 0$ for $d'_r(\mathcal{C}) + 1 \le i \le n$. This further implies that $\forall \mathbf{x} \in D, x \in \big\langle \{\delta_i^T, 1 \le i \le d'_r(\mathcal{C})\} \big\rangle$. Therefore,

$$d_r(\mathcal{C}, F) \le d'_r(\mathcal{C}). \tag{5.76}$$

On the other hand, let $\mathrm{W} \subset \{1, 2, \ldots, n\}$ and $|\mathrm{W}| = d_r(\mathcal{C}, F)$ such that $\langle \{\delta_i, i \in \mathrm{W}\} \rangle$ contains some subcode D of C with dimension r. Without loss of generality, assume $\mathrm{W} = \{1, 2, \ldots, d_r(\mathcal{C}, F)\}$. This implies $\forall \mathbf{x} \in D, x_i = 0$ where $d_r(\mathcal{C}, F) + 1 \le i \le n$. This further implies

$\mathcal{X}(D) \subset \{1, 2, \ldots, d_r(\mathcal{C}, F)\}$ and $|\mathcal{X}(D)| \leq d_r(\mathcal{C}, F)$. Therefore,

$$d'_r(\mathcal{C}) \leq d_r(\mathcal{C}, F). \tag{5.77}$$

According to Theorem 5.2, the network generalized Hamming weight can be regarded as a generalized Singleton bound for the classical point-to-point channel. In particular, for $r = 1$, we have $d_1(\mathcal{C}, F) \leq n - k + 1$, which is precisely the Singleton bound in classical algebraic coding theory.

5.6 Conclusion

In this chapter, we define the network generalized Hamming weight of a linear block code with respect to a fixed set of global encoding kernels of a given linear network code, which is a network generalization of the generalized Hamming weight for the classical point-to-point communication channel. Based on our definition, we obtain the network generalized Singleton bound and prove its achievability of the generalized Singleton bound. In addition, the network generalized Hamming weight can completely characterize the security performance of linear block code when it is applied in conjunction with a linear network code on a CSWN. Moreover, the construction approach of secure network code in [5] and [7] can be regarded as a construction method of an NMDS code for any given linear network code. Finally, a one-pass construction of secure linear network coding scheme for the network with multicast capacity n is also given. A linear secure network code which can multicast data securely to the predefined sink nodes at the highest possible rate of k at the present of an adversary that can eavesdrop any set of $n - k$ channels can be constructed.

□ **End of chapter.**

Chapter 6

Conclusion

This thesis explores the security and error-correcting issues in the area of linear network coding. In Chapter 4, we first formulate the network coding problem with security and error-correction simultaneously. An algorithm for constructing a deterministic secure error-correcting (SEC) network code is proposed. We have shown that in the presence of malicious parties, by combining the ideas of secure network coding and error correction network coding, information can be multicast with complete secrecy (i.e., with information theoretic security) and error tolerability at the rate of $m - 2d - k$, where m is the minimum of the maxflows from the source node to the sink nodes, and k and d are the maximum number of channels the adversary can eavesdrop and contaminate, respectively. By utilizing Han's inequalies [47], $m - 2d - k$ is also shown to be an upper bound on the multicast rate of secure error-correcting network code in the presence of an adversary that can inject d errors and eavesdrop k channels. However, it is not clear whether this bound continues to hold for nonlinear network codes. By applying the so constructed network code to create a temporary secure channel, we further propose different schemes that can achieve the higher multicast rate of $m - d$ with high probability. At last, we also show that with feedback channels from the sink nodes to the source node, depending on the maximum dimension of errors the adversary can impose upon everh sink nodes, it is possible to boost the multicast rate beyond $m - d$ without further modification of the existing network code.

In Chapter 5, we extend the notion of generalized Hamming weight for classical linear block code proposed by Wei [9] to linear network codes by proposing the *network generalized Hamming weight (NGHW)* for a given network with respect to a fixed set of global encoding kernels. The basic properties of the NGHW are studied. We also extend the generalized Singleton bound in [9] to linear network codes. We further show that the NGHW can be used as a tool to characterize the security performance of a linear code on the communication system on a wiretap network (CSWN) [5]. We also introduce the idea of Network Maximum Distance Separation code (NMDS code) by extending the notion of Maximum Distance Separation code in classical algebraic coding theory. We prove that NMDS codes play an important role in minimizing the information that an eavesdropper can obtain from the network. In addition, a one-pass construction of a secure network code is given.

□ **End of chapter.**

Appendix A

Coset Coding

Let $\mathcal{C}$ be a subcode of $\mathbb{F}_q^n$ and $\mathbf{x}_1 \in \langle G_M \rangle$. Then,

$$\mathbf{x}_1 + \mathcal{C} = \{\mathbf{x}_1 + \mathbf{x}' : \mathbf{x}' \in \langle G_M \rangle\}. \tag{A.1}$$

For every subcode $\mathcal{C}$ of $\mathbb{F}_q^n$, we will show that the collection of sets, $\mathbf{x}_1 + \mathcal{C}, \forall \mathbf{x}_1 \in \langle G_M \rangle$ are left cosets of $\mathbb{F}_q^n$ under the addition operation, and all together they form a partition of $\mathbb{F}_q^n$: every element of $\mathbb{F}_q^n$ belongs to one and only one of $\mathbf{x}_1 + \mathcal{C}$.

Proof. $\forall \mathbf{x}_1, \mathbf{x}_2 \in \langle G_M \rangle$ where $\mathbf{x}_1 \neq \mathbf{x}_2$, if there exist $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$ s.t.

$$\mathbf{x}_1 + \mathbf{c}_1 = \mathbf{x}_2 + \mathbf{c}_2 \tag{A.2}$$

then

$$\mathbf{x}_1 - \mathbf{x}_2 = \mathbf{c}_2 - \mathbf{c}_1. \tag{A.3}$$

That is, there exists $\mathbf{x} = \mathbf{x}_1 - \mathbf{x}_2 \in \langle G_M \rangle$ s.t. $\mathbf{x} \in \mathcal{C}$. This contradicts the fact that G_M and G_C together form a $n \times n$ full-rank matrix. Therefore,

$$(\mathbf{x}_1 + \mathcal{C}) \cap (\mathbf{x}_2 + \mathcal{C}) = \emptyset. \tag{A.4}$$

In addition, since G_M and G_C together form a $n \times n$ full-rank matrix,

$$\bigcup_{\mathbf{x} \in \langle G_M \rangle} (\mathbf{x} + \mathcal{C}) = \mathbb{F}_q^n. \tag{A.5}$$

Therefore, $\mathbf{x} + \mathcal{C}, \forall \mathbf{x} \in \langle G_M \rangle$ are left cosets of $\mathbb{F}_q^n$ and form a partition of $\mathbb{F}_q^n$. □

Appendix B

Lower Bound on the Information Leakage

Summary

Here we calculate the lower bound on the information of the source that the eavesdropper can obtain despite the coding scheme being used to multicast information.

Given a graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ with maxflow n, we assume that information is multicasting from the source node s to a set of sink nodes $\mathcal{T}$ at rate k, where $k \leq n$. Let the maxflow from source node s to a sink node $t \in \mathcal{T}$ be n. There exists a set of channels $E \subset \mathcal{E}$, with $|E| = n$, which forms a cut between s and t. Let τ, where $n - k \leq \tau \leq n$, be the number of channels that the eavesdropper can wiretap. Let E_1 and E_2 be two disjoint subsets of E such that $E_1 \cup E_2 = E$ with $|E_1| = n - \tau$ and $|E_2| = \tau$. We further assume that now the eavesdropper choose to wiretap E_2.

Let S be the random variable denoting the information source, Y_1 be the random variable denoting the message transmitting in E_1 and Y_2 be the random variable denoting the message transmitting in E_2. $H(\cdot|\cdot)$, $H(\cdot)$, and $I(\cdot;\cdot|\cdot)$ will be used to denote conditional entropy, entropy, and conditional mutual information respectively. Then,

$$H(S|Y_1, Y_2) = H(S|Y_2) - I(S; Y_1|Y_2). \tag{B.1}$$

Since E is a cut between s and t, $H(S|Y_1, Y_2) = 0$, so that

$$0 = H(S|Y_2) - I(S; Y_1|Y_2), \tag{B.2}$$

or

$$0 = H(S) - I(S; Y_2) - I(S; Y_1|Y_2), \tag{B.3}$$

where $I(S; Y_2)$ is regarded as the amount of information of the source that the eavesdropper can obtained by wiretapping E_2.

By rearranging the terms in (B.3), we can then obtain

$$\begin{aligned} I(S; Y_2) &= H(S) - I(S; Y_1|Y_2) && \text{(B.4)} \\ &\geq H(S) - H(Y_1) && \text{(B.5)} \\ &\geq k - (n - \tau) && \text{(B.6)} \\ &= k + \tau - n. && \text{(B.7)} \end{aligned}$$

□ **End of chapter.**

Bibliography

[1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network Information Flow," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp 1204-1216, Jul. 2000.

[2] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear Network Coding," *IEEE Trans. Inform. Theory*, vol. 49, no. 2, pp 371-381, Feb. 2003.

[3] R. W. Yeung and Z. Zhang, "Distributed source coding for satellite communications, " *IEEE Trans. Inform. Theory*, vol. 45, pp 1111-1120, 1999.

[4] R. Koetter and M. Médard, "An algebraic approach to network coding," in *Proc.* IEEE INFOCOM, 2002.

[5] N. Cai and R. W. Yeung,"Secure Network Coding", in *Proc.* 2002 IEEE International Symposium on Information Theory, June 2002.

[6] N. Cai and R. W. Yeung,"A Secure Condition for Multi-Source Linear Network Coding Network Coding", in *Proc.* 2007 IEEE International Symposium on Information Theory, June 2007.

[7] S. Y. E. Rouayheb and E. Soljanin, "On Wiretap Networks II," in *Proc.* 2007 IEEE International Symposium on Information Theory, June 2007.

[8] L. H. Ozarow and A. D. Wyner,"Wire-tap-channel II," AT& T Bell Labs Technical Journal, Vol63, pp.2135-2157, 1984.

[9] V. K. Wei,"Generalized Hamming Weight for Linear Codes," *IEEE Trans. Inform. Theory*,vol. 37 , no. 5, pp 1412-1418, Sep.1991.

[10] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, *Network Coding Theory*, now Publishers, 2005.

[11] S. Jaggi, P. Sanders and etc."Polynomial time algorithms for multicast network code construction," *IEEE Trans. Inform. Theory*, vol.51, no. 6, pp.1973-1982, June 2005.

[12] J. Feldman, T. Malkin, C. Stein, and R. A. Servedio, "On the Capacity of Secure Network Coding," in *Proc.* 42nd Annual Allerton Conference on Communication, Control, and Computing, September 2004.

[13] R. W. Yeung and N. Cai, "On the optimality of a construction of a secure network codes," in *Proc.* 2008 IEEE International Symposium on Information Theory, July 2008.

[14] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc.* the National Computer Conference, 48: 313-317, 1979.

[15] A. Shamir, "How to share a secret," *Comm.* ACM, 22: 612-613, 1979.

[16] T. Ho, B. Leong, R. Koetter, M. Médard, M. Effros, and D. R. Karger, "Byzantine modification detection in multicast networks using packetized network coding," in *Proc.* 2004 IEEE International Symposium on Information Theory, June 2004.

[17] S. Jaggi, M. Langberg, T. Ho, and M. Effros, "Correction of adversarial errors in networks," in *Proc.* 2005 IEEE International Symposium on Information Theory, July 2005.

[18] N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc.* 2002 IEEE Information Theory Workshop, 2002.

[19] R. W. Yeung and N. Cai, "Network error correction, part I: basic concepts and upper bounds," *Communications in Information and Systems,* vol. 6, no. 1, pp. 19-36, 2006.

[20] N. Cai and R. W. Yeung, "Network error correction, part II: lower bounds," *Communications in Information and Systems,* vol. 6, no. 1, pp.37-54, 2006.

[21] Z. Zhang, "Network error correction coding in packetized networks," in *Proc.* 2006 IEEE Information Theory Workshop, Oct. 2006.

[22] S. Yang and R. W. Yeung, "Characterizations of Network Error Correction/Detection and Erasure Correction," in *Proc.* Netcod, Jan. 2007.

[23] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient network coding in the presence of byzantine adversaries," in *Proc.* IEEE INFOCOM, 2007.

[24] S. Yang, C. K. Ngai and R. W. Yeung, "Construction of Linear Network Codes that Achieve a Refined Singleton Bound," in *Proc.* 2007 IEEE International Symposium on Information Theory, Nice.

[25] S. Jaggi, and M. Langberg, "Resilient network codes in the presence of eavesdropping Byzantine adversaries," in *Proc.* 2007 IEEE International Symposium on Information Theory, 2007.

[26] T. Ho, M. Médard, J. Shi, M. Effros and D. R. Karger, "On Randomized Network Coding," in *Proc.* 41st Annual Allerton Conference on Communication Control and Computing, Oct. 2003.

[27] S. Yang, and R. W. Yeung, "Refined Coding Bounds for Network Error Correction," in *Proc.* 2007 IEEE Information Theory Workshop, Bergen, Noway, 2007.

[28] L. K. Ford, Jr. and D. K. Fulkerson, *Flows in Networks,* Princeton University Press, Princeton, New Jersey, 1962.

[29] C. H. Papadimitriou, and K. Steiglitz, *Combinatorial optimization: Algorithms and c1omplexity*, 1982.

[30] C. E. Shannon, “Communication theory of secrecy systems”, Bell Sys. Technical Journal 28, pp. 656-715, 1949.

[31] R. W. Yeung, *A First Course in Information Theory,* Kluwer Academic/Plenum Publishers, 2002.

[32] D. S. Lun, M. Médard, and R. Koetter, “Efficient operation of wireless packet networks using network coding,” in *Proc.* International Workshop on Convergent Technologies (IWCT), 2005.

[33] S. Katti, D. Katabi, W. Hu, H. S. Rahul, and M. Médard, “The importance of being opportunistic: Practical network coding for wireless environments,” in *Proc.* 43rd Annual Allerton Conference on Communication, Control, and Computing, 2005.

[34] S. Katti, H. Rahul, D. Katabi, W. H. M. Médard, and J. Crowcroft, “Xors in the air: Practical wireless network coding,” in *Proc.* ACM SIGCOMM, 2006.

[35] J. E. Wieselthier, G. D. Nguyen, and A. Ephremides, “On the construction of energy-efficient broadcast and multicast trees in wireless networks,” in *Proc.* IEEE INFOCOM, volume 2, pages 585-594, 2000.

[36] C. Gkantsidis and P. Rodriguez,“Network Coding for Large Scale Content Distribution,” in *Proc.* IEEE INFOCOM, 2005.

[37] A. Jiang, “Network Coding for Joing Storage and Transmission with Minimum Cost,” in *Proc.* 2006 IEEE International Symposium on Information Theory, 2006.

[38] E. R. Berlekamp, *Block coding for the binary symmetric channel with noiseless, delayless feedback,” in Error Correcting Codes,* Wiley, New York, 1968.

[39] R. E. Blahut, *Theory and Practice of Error Control Codes,* Addison-Wesley, Reading, Massachusetts, 1983.

[40] S. Lin and D. J. Costello, Jr., *Error Control Coding: Fundamentals and Applications,* Prentice-Hall, Englewood Cliffs, New Jersey, 1983.

[41] S. B. Wicker, *Error Control Systems for Digital Communication and Storage,* Prentice-Hall, Englewood Cliffs, New Jersey, 1995.

[42] B. Bollobas, *Graph Theory, An Introductory Course,* Springer-Verlag, 1979.

[43] E Erez and M. Feder, "Convolutional Network Codes", in *Proc.* 2004 IEEE International Symposium on Information Theory, 2004.

[44] C. Fragouli and E. Soljanin, "A connection between network coding and convolutional codes," IEEE International Conference on Communications, 2004.

[45] E. Erez and M. Feder, "Convolutional network codes for cyclic networks," NetCod 2005, Italy, 2005.

[46] S.-Y. R. Li and S. T. Ho, "Ring-Theoretic Foundation of Convolutional Network Coding," NetCod 2008, Hong Kong, 2008.

[47] T. S. Han, "Nonnegative entropy measures of multivariate symmetric correlations," Info. Contr., 36: 133-156, 1978.